

COOPERATION AND SERVICE AGREEMENT

This Cooperation and Service Agreement (the “Agreement”) is entered into as of _____ (the “Effective Date”) between PayByPhone US Inc., a provider of enhanced mobile commerce solutions, a Delaware corporation with its address at 48 Wall Street, Suite 1100, New York, New York 10005 (“PayByPhone”) and City of Kirkland, a provider of parking services with its address at: 123 Fifth Ave. Kirkland, WA. 98033 (“Client”).

RECITALS

The objective between PayByPhone and Client provided for in this Agreement is for PayByPhone to provide wireless applications to enhance the payment process for parking at parking facilities and metered parking stalls owned and/or managed by Client, described in more detail in Appendix A (each address listed is a “Parking Location”). PayByPhone mobile commerce solutions will also provide Client with a management information system, including real-time operation and transaction reports.

AGREEMENT

Section 1 THE PAYBYPHONE MOBILE PAYMENT PLATFORM AND APPLICATIONS

1.1 PAYBYPHONE MOBILE PAYMENT APPLICATION

PayByPhone agrees to roll out the PayByPhone mobile payment service for use at Client’s managed and owned parking facilities as agreed upon by PayByPhone and Client, to allow for consumers to pay for the use of Client’s parking facilities through personal wireless devices (e.g., cellular telephones) or other wireless systems. QR code access to the payment service is not included.

1.2 PAYBYPHONE MANAGEMENT INFORMATION SYSTEM

PayByPhone will operate and manage a software application for Client that will provide near real time information and management reports on the transactions conducted utilizing the PayByPhone mobile payment service (the “Portal”). PayByPhone will host the Portal on its network. Client will access the Portal through a browser-based program installed on Client’s computer hardware.

1.3 COMPUTER, NETWORKING AND TELECOMMUNICATION SYSTEMS

PayByPhone or its parent, PayByPhone Technologies Inc. will own or possess, and will operate and maintain, all computer and networking hardware and software and data required to operate the PayByPhone mobile payment services service as contemplated in this Agreement, other than Client’s existing computer and telecommunications systems.

1.4 MOBILE PAYMENT SERVICE ENFORCEMENT

Client agrees to supply Wireless Devices to employees in the field to provide real time confirmation of validly parked vehicles.

1.5 REPORTS

PayByPhone will provide Client with a set of standard self-serve reports in the Portal. Any changes or customizations to the standard set of reports will be subject to PayByPhone’s prior approval and then-current PayByPhone professional services fees.

See https://www.paybyphone.com/pdf/us/pbp_professionalservicesamplerates.pdf for sample rates.

Section 2 FEES AND PAYMENTS

2.1 PRICING AND PAYMENT

Client agrees to pay the fees, as outlined in Appendix A. All amounts payable hereunder are exclusive of any and all taxes, including taxes applicable on fees paid by the consumer, and Client is responsible for payment of such taxes. All prices are stated, and Client shall pay, in US dollars. Payment is due within 30 days of invoicing. PayByPhone

may, acting reasonably, increase any fees outlined in Appendix A, not more often than once in a calendar year, to adjust for inflation and any increase in the cost of PayByPhone providing the services to Client, however, any increase shall not exceed 4% in any calendar year.

2.2 MERCHANT ACCOUNT

Merchant account refers to Client's merchant account set up with Client's acquiring bank. PayByPhone will cover the cost of linking one (1) Client merchant account with PayByPhone's gateway provider. Client agrees to cover the cost of merchant account updates including all third party fees and then-current PayByPhone professional services fees. See https://www.paybyphone.com/pdf/us/pbp_professionalservicesamplerrates.pdf for sample rates.

2.3 TRANSACTION TESTING

PayByPhone reserves the right to execute test transactions from time to time to ensure top performance of the system and account. PayByPhone may execute up to ten test transactions per month without adjusting the Client invoice.

2.4 THIRD PARTY INTEGRATION

In the event that system changes (such as upgrades) by a third party impact the PayByPhone integration with Client sub-systems such as enforcement, PayByPhone will notify Client, in advance, with a cost estimate of any such integration costs and seek approval.

2.5 EXCLUSIVITY

The parties expressly acknowledge that Client currently engages, and/or may in the future, at its option, add, other providers of mobile parking payment applications ("Third Party Providers"), through contracts for the same parking facilities and metered stalls covered by this Agreement.

Section 3 MARKETING, PROMOTION AND USER EDUCATION

3.1 SIGNAGE

Client agrees to use the PayByPhone decals and signs already installed at the Parking Locations as of the Effective Date where PayByPhone services are provided to the Client. All additional and replacement signage is at Client's cost. Client agrees to either use PayByPhone's standard signage template or ensure that its non-standard signage complies with all PayByPhone's marketing and branding guidelines (available on request). Client shall not modify PayByPhone's logos, fonts, colours, design, and other brand/marketing related items without PayByPhone's prior written consent and approval. In the event Client requests that PayByPhone produce non-standard signage for Client, such customization work will be subject to PayByPhone's prior approval and then-current PayByPhone professional services fees. See https://www.paybyphone.com/pdf/us/pbp_professionalservicesamplerrates.pdf for sample fees. Client will be responsible for installation of all additional and replacement decals and signs at the Parking Locations.

3.2 MARKETING EVENTS

PayByPhone may conduct on-site marketing events and campaigns for its service, whereby PayByPhone will inform parking lot consumers of the availability of the PayByPhone mobile payment services as well as any promotions available, with the knowledge and approval of Client which is not to be unreasonably withheld consistent with all applicable law and permitting requirements.

3.3 CLIENT TRAINING

PayByPhone will provide initial training to Client using a "Train the Trainer" (the "Client Trainer") model on the self-served PayByPhone Service Management Interface (SMI). The said Client Trainer will, at its own expense, train its staff and employees, including patrollers, to operate the mobile payment services and related applications and technology. Additional training sessions are available at the then current professional services rates. See https://www.paybyphone.com/pdf/us/pbp_professionalservicesamplerrates.pdf for sample rates.

Section 4 INTELLECTUAL PROPERTY

4.1 INTELLECTUAL PROPERTY RIGHTS

- 4.1.1 The parties acknowledge and agree that any trademarks, patents, trade names, logos, trade dress, domain names, copyrights or licenses therein, or other enforceable intellectual property rights and whether in hard or electronic copy (collectively “Intellectual Property”) belonging to the other party, given to them under this Agreement is and shall remain the property of that party for the duration of the Term of this Agreement.
- 4.1.2 Except as expressly stated, nothing in this Agreement shall be deemed or interpreted to convey, transfer or assign any Intellectual Property rights to the other party.
- 4.1.3 Each party reserves the right to approve in advance the use of its Intellectual Property by the other party in each and every instance.
- 4.1.4 Upon termination of this Agreement for any reason the parties will use reasonable endeavours to ensure that all such Intellectual Property and material are removed from display and/or destroyed at the request of the other party save where such Intellectual Property is held by the parties in compliance with any statutory obligations and/or the maintenance of proper records.
- 4.1.5 The parties undertake that they have all necessary permissions, licenses and rights to use the Intellectual Property of third parties for the purposes of this Agreement.
- 4.1.6 To the extent permitted by law, each party shall indemnify (for the purposes of this clause, the “Indemnifying Party”) the other (for the purposes of this clause the “Indemnified Party”) against all actions, claims, proceedings, costs and expenses (including reasonable legal fees) arising from any actual infringement of Intellectual Property rights of whatever nature insofar as these relate to the Intellectual Property rights developed and owned by the Indemnifying Party or licensed to the Indemnified Party which claims, actions or proceedings arise as a result of the Indemnified Party’s use of any of the Services, except that the indemnity shall not apply to any actions, claims or proceedings which are attributable to any breach of contract or negligent act or omission on the part of the Indemnified Party or where such actions, claims or proceedings relate to any developments of the services carried out by or at the request of the Indemnified Party except where the Indemnifying Party knew or ought to have known that such development of the services requested by the Indemnified Party would result in an infringement of Intellectual Property rights.
- 4.1.7 The Indemnified Party shall notify the Indemnifying Party in writing of any such action, claim or proceeding and shall not make any admission unless the Indemnifying Party gives prior written consent.
- 4.1.8 At the Indemnifying Party’s request and expense, the Indemnified Party shall permit the Indemnifying Party to conduct all negotiations and litigation. The Indemnified Party shall give all assistance as the Indemnifying Party may reasonably request and the Indemnifying Party shall pay the Indemnified Party’s costs and expenses so incurred.
- 4.1.9 The Indemnifying Party may, at its expense: (i) obtain a license to enable the Indemnified Party to continue to use the Services, or (ii) modify or replace the Services to avoid any alleged or actual infringement or breach, or (iii) terminate the provision of the affected elements of the Services. Where the Indemnifying Party exercises options (i) or (ii) the functionality of such modification or replacement shall not materially affect the performance of the Services.

4.2 CLIENT INFORMATION

- 4.2.1 “Client Data” means all data provided directly by the Client to PayByPhone in relation to this Agreement, including Client’s parking rates, Client’s identifiers for Parking Locations and parking stalls, merchant account information, enforcement equipment and practices, and parking policies.

- 4.2.2 During the term of this Agreement and for such time after as not expressly prohibited, PayByPhone may obtain, store and use such Client Data for any lawful purpose, including without limitation providing and improving services under this Agreement, so long as it complies with applicable data protection laws, contractual obligations and any other applicable requirements with respect to the Client Data. PayByPhone shall retain exclusive ownership of all rights in any derivative data it develops based on Client Data.
- 4.2.3 Following termination of this Agreement, PayByPhone will, at Client's written request, return to Client or destroy all Client Data and copies thereof. Notwithstanding the foregoing, PayByPhone shall be permitted to retain such copies of, or any computer records or files containing, the Client Data: (a) that has been archived by PayByPhone's automatic electronic archiving and back-up procedures, to the extent created and retained in a manner consistent with PayByPhone's standard archiving and back-up procedures; and (b) to the extent required by applicable law.

4.3 CUSTOMER INFORMATION

- 4.3.1 The parties will share information and data directly relating to drivers' parking sessions through the PayByPhone service at the Parking Locations ("Parking Sessions") and as may be required by the Client for parking enforcement, fines, and proceedings ("Transaction Data"). Transaction Data may include vehicle license plate, parking session date, time, duration, zone number and amount paid, details of parking fines/violation notices, and parking session details obtained through customer service centre, and does not include User Profile Data (defined below).
- 4.3.2 In using, sharing, or otherwise processing Transaction Data, PayByPhone and Client must comply with applicable data protection laws, contractual obligations and any other applicable requirements. Each party is responsible to the PayByPhone service users and other third parties for its respective use, sharing and processing of Transaction Data, whether it performs such use, sharing and processing directly or through third parties. Each party acts as a "data controller" with respect to Transaction Data for the purposes any privacy legislation that uses that concept and is applicable to the party's activities. Each party agrees to provide such assistance as is reasonably required to enable the other party to comply with the applicable data protection laws.
- 4.3.3 Any information about or with respect to PayByPhone service users that is not related to parking sessions at the Parking Locations, including without limitation, information provided by users upon registration for a PayByPhone account and data about the user's activity in the PayByPhone account or the PayByPhone applications ("User Profile Data") shall be exclusively owned by PayByPhone. PayByPhone shall retain exclusive ownership of all rights in any derivative data it develops based on Transaction Data and User Profile Data.

4.4 PAYBYPHONE'S SERVICES TO CUSTOMERS

The parties acknowledge that PayByPhone service users hold the PayByPhone account under terms of service established by PayByPhone. Under these terms of service, PayByPhone may offer users an option to receive service communications by SMS text ("SMS Communications"), including reminders to extend a parking session and confirmations of successful registration for a parking session. Client agrees that, at any time during the Term, PayByPhone may charge any users who opt into these services a fee ("SMS Fee") for each SMS Communication sent by PayByPhone with respect to an initial parking session or extension of a parking session and may set the amount of the SMS Fee with reference to the cost PayByPhone incurs in delivering this optional service. At the time of entering into this Agreement, the SMS Fee is equal to \$0.15, inclusive of taxes payable by the user. PayByPhone will provide Client with 30 day written notice of an increase in the amount of the SMS Fee. PayByPhone shall be responsible for any taxes applicable to the SMS Fees. PayByPhone records will be conclusive evidence with respect to the amount of SMS Fees collected during a billing period. The SMS Fees will be added to the total charged to the user in respect of a parking session or extension of a parking session.

Unless under the terms of the Agreement PayByPhone is designated as the merchant of record for parking fees paid using PayByPhone mobile payment service, PayByPhone and Client agree to designate Client as

the merchant of record for any SMS Fees only. In that case, Client will collect PayByPhone's SMS Fees and remit to PayByPhone. Remittance will be made via electronic payment or cheque and may be included in the amount that also includes fees payable by Client to PayByPhone under this Agreement.

Section 5 TERM AND TERMINATION

5.1 TERM AND RENEWAL

5.1.1 This Agreement shall enter into force on the Effective Date and shall remain in force and effect for a period of three consecutive years (the "Initial Term") from the Effective Date.

5.1.2 Upon the termination of the Initial Term, the Agreement will automatically renew for one (1) or more additional terms of one (1) year each (each a "Renewal Term"), unless either party gives the other party at least ninety (90) days prior written notice of its intent to not renew the Agreement before the end of the then-current Term. If notice is provided at least ninety (90) days prior to the Renewal Term, the parties shall terminate the Agreement, at no additional cost to either party. The Initial Term and all Renewal Terms, if any, shall collectively be referred to as the "Term".

5.2 TERMINATION

Should a party breach a material term and such breach remains uncorrected for thirty (30) days after receipt of a notice by the breaching party, the non-breaching party may, in addition to all other remedies available at law, terminate this Agreement by providing written notice to the breaching party, without further obligation provided, however, that if the nature of the breach is such that it cannot be reasonably cured within such thirty (30) day period, the breaching party will not be deemed in default of this Agreement so long as such party commences efforts to effect a cure and is diligently pursuing such efforts. Provided, further, that if the breach is as a result of the non-payment of any fee, the non-breaching party may terminate this Agreement if such breach remains uncorrected for ten (10) days after the breaching party's receipt of notice of such breach.

Section 6 REPRESENTATIONS AND WARRANTIES

6.1 MUTUAL REPRESENTATIONS AND WARRANTIES

Each party represents and warrants to the other that:

- i) it has the full corporate right and authority, and possesses all licenses, permits, authorizations and rights to intellectual property, necessary to enter into and perform this Agreement;
- ii) its entry into and performance of this Agreement do not and will not conflict with or result in a breach or violation of any agreement or order by which it is bound; and
- iii) this Agreement constitutes its legal, valid and binding obligations enforceable against it in accordance with the terms of this Agreement.

Section 7 DISCLAIMER, INDEMNIFICATION, LIMITATION OF LIABILITY AND INSURANCE

7.1 DISCLAIMER

Except as expressly set forth in this agreement, PayByPhone does not make, and hereby specifically disclaims, any representations or warranties, express or implied, regarding the PayByPhone mobile payment services, including any implied warranties of title, or non-infringement. Client acknowledges that the PayByPhone mobile payment services and services furnished by PayByPhone under this agreement (including, without limitation, any servers or other hardware, software, applications and any other items used or provided by PayByPhone or any third parties in connection with providing access to or hosting any of the foregoing or the performance of any services by PayByPhone under this agreement) are provided by PayByPhone "as is".

PayByPhone represents and warrants that all contracted services set forth in Appendix A will be provided during the Term.

7.2 INDEMNIFICATION

To the extent permitted by law and subject to Section 7.3, each party (the “Indemnifying Party”) will defend, indemnify and hold harmless the other party (the “Indemnified Party”) from and against any and all third party claims, actions, losses (collectively, “Losses”) resulting from or arising out of the Indemnifying Party’s breach of any representation, warranty or other obligation set forth in this Agreement. The Indemnified Party shall not be entitled to be so indemnified unless it has given the Indemnifying Party prompt written notice of any Losses, afforded the Indemnifying Party the opportunity to assume sole control over the defence and settlement, if applicable, of the Losses, and provided the Indemnifying Party (at the Indemnifying Party’s expense) all relevant information, assistance and authority to enable the Indemnifying Party to perform its obligations hereunder. The Indemnifying Party shall not settle any Losses without the Indemnified Party’s written consent, which shall not be unreasonably withheld.

7.3 LIMITATION OF LIABILITY

In no event shall any party be liable for consequential, special, indirect or incidental damages, including but not limited to any damages resulting from loss of use or profits arising out of or in connection with this agreement, whether in an action based on contract, tort (including negligence) or any other legal theory, even if the party has been advised of the possibility of such damages.

7.4 PARKING RATES

Client will be given access to parking rate data in order to confirm the parking rates at each Parking Location via the Portal. PayByPhone will make every attempt at ensuring the rates are configured correctly; upon completion of each Parking Location setup, it is the Client’s responsibility to ensure all rates are configured correctly. Failing to do so shall exclude PayByPhone from any liability. Client shall implement any parking rate changes via the Portal following the Parking Location setup. In the event Client requests that PayByPhone configure the parking rate changes after the Parking Location setup, Client shall provide PayByPhone with sufficient notice of the rate changes and such work will be subject to PayByPhone’s prior approval and then-current PayByPhone professional services fees. See https://www.paybyphone.com/pdf/us/pbp_professionalservicesamplerates.pdf for sample fees.

7.5 LIABILITY INSURANCE COVERAGE

PayByPhone (or “Vendor”) shall procure and maintain for the duration of the Agreement, insurance against claims for injuries to persons or damage to property which may arise from or in connection with the performance of the work hereunder by the Vendor, its agents, representatives, or employees. A failure to obtain and maintain such insurance or to file required certificates and endorsements shall be a material breach of this Agreement.

Vendor’s maintenance of insurance as required by the agreement shall not be construed to limit the liability of the Vendor to the coverage provided by such insurance, or otherwise limit the City’s recourse to any remedy available at law or in equity.

7.5.1 MINIMUM SCOPE OF INSURANCE

Vendor shall obtain insurance of the types described below:

1. Commercial General Liability insurance shall be as least as broad as ISO occurrence form CG 00 01 and shall cover liability arising from premises, operations, stop-gap independent contractors and personal injury and advertising injury. The City shall be named as an additional insured under the Vendor’s Commercial General Liability insurance policy with respect to the work performed for the City using an additional insured endorsement at least as broad as ISO CG 20 26.
2. Workers’ Compensation coverage as required by the Industrial Insurance laws of the State of Washington.
3. Professional Liability insurance appropriate to the Vendor’s profession.
4. Network Security (Cyber) and Privacy Insurance shall include, but not be limited to, coverage, including defense, for the following losses or services:

Liability arising from theft, dissemination, and/or use of City confidential and personally identifiable information, including but not limited to, any information about an individual maintained by or on behalf of

the City, including (i) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information regardless of how or where the information is stored or transmitted. Network security liability arising from (i) the unauthorized access to, use of, or tampering with computer systems, including hacker attacks; or (ii) the inability of an authorized Third Party to gain access to supplier systems and/or City Data, including denial of service, unless caused by a mechanical or electrical failure; (iii) introduction of any unauthorized software computer code or virus causing damage to the City or any other Third Party Data.

Lawfully insurable fines and penalties resulting or allegedly resulting from a Data breach.

Event management services and first-party loss expenses for a Data breach response including crisis management services, credit monitoring for individuals, public relations, legal service advice, notification of affected parties, independent information security forensics firm, and costs to re-secure, re-create and restore Data or systems.

For purposes of this insurance subsection, the terms Third Party and Data are defined in Section XI.

7.5.2 MINIMUM AMOUNTS OF INSURANCE

Vendor shall maintain the following insurance limits:

1. Commercial General Liability insurance shall be written with limits no less than \$1,000,000 each occurrence, \$2,000,000 general aggregate.
2. Professional Liability insurance shall be written with limits no less than \$1,000,000 per claim and \$1,000,000 policy aggregate limit.
3. Network Security (Cyber) and Privacy Insurance shall be written with limits no less than \$1,000,000 per claim, \$2,000,000 policy aggregate for network security and privacy coverage, \$100,000 per claim for regulatory action (fines and penalties), and \$100,000 per claim for event management services.

7.5.3 OTHER INSURANCE PROVISIONS

The insurance policies are to contain, or be endorsed to contain, the following provisions for Commercial General Liability insurance:

1. The Vendor's insurance coverage shall be primary insurance as respects the City. Any insurance, self-insurance, or self-insured pool coverage maintained by the City shall be excess of the Vendor's insurance and shall not contribute with it.
2. The Vendor shall provide the City and all Additional Insureds for this services with written notice of any policy cancellation, within two business days of their receipt of such notice.

7.5.4 ACCEPTABILITY OF INSURERS

Insurance is to be placed with insurers with a current A.M. Best rating of not less than A:VII.

1. Verification of Coverage

Vendor shall furnish the City with original certificates and a copy of the amendatory endorsements, including but not necessarily limited to the additional insured endorsement, evidencing the insurance requirements of the Vendor before commencement of the services.

2. Failure to Maintain Insurance

Failure on the part of the Vendor to maintain the insurance as required shall constitute a material breach of agreement, upon which the City may, after giving five business days' notice to the Vendor to correct the breach, immediately terminate the agreement or, at its discretion, procure or renew such insurance and pay any and all premiums in connection therewith, with any sums so expended to be repaid to the City on demand, or at the sole discretion of the City, offset against funds due the Vendor from the City.

3. City Full Availability of Vendor Limits

If the Vendor maintains higher insurance limits than the minimums shown above, the City shall be insured for the full available limits of Commercial General and Excess or Umbrella liability maintained by the Vendor, irrespective of whether such limits maintained by the Vendor are greater than those required by this agreement or whether any certificate of insurance furnished to the City evidences limits of liability lower than those maintained by the Vendor.

7.6. SAFEGUARDING OF PERSONAL INFORMATION

7.6.1 DEFINITIONS. The following definitions shall have the assigned meaning for this section.

1. **"Data"** means all information, whether in oral or written (including electronic) form, created by or in any way originating with City and End Users, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with City and End Users, in the course of using and configuring the Services provided under this Agreement, and includes City Data, End User Data, and Personal Information.
2. **"Data Compromise"** means any actual or reasonably suspected unauthorized access to or acquisition of computerized Data that compromises the security, confidentiality, or integrity of the Data, or the ability of City to access the Data.
3. **"End User"** means the individuals (including, but not limited to employees, authorized agents, students and volunteers of City; Third Party consultants, auditors and other independent contractors performing services for City; any governmental, accrediting or regulatory bodies lawfully requesting or requiring access to any Services; customers of City provided services; and any external users collaborating with City) authorized by City to access and use the Services provided by Contractor under this Agreement.
4. **"Third Party"** means persons, corporations and entities other than Consultant, or any of their employees, contractors or agents.
 - A. The Vendor shall not use or disclose Personal Information, as defined in RCW 19.255.010, in any manner that would constitute a violation of federal law or applicable provisions of Washington State law. Vendor agrees to comply with all federal and state laws and regulations, as currently enacted or revised, regarding Data security and electronic Data interchange of Personal Information.

The Vendor shall ensure its directors, officers, employees, subcontractors or agents use Personal Information solely for the purposes of accomplishing the services set forth in the Agreement.

The Vendor shall protect Personal Information collected, used, or acquired in connection with the Agreement, against unauthorized use, disclosure, modification or loss.

The Vendor and its sub-consultants and agents agree not to release, divulge, publish, transfer, sell or otherwise make Personal Information known to unauthorized persons without the express, prior written consent of the City or as otherwise authorized by law.

The Vendor agrees to implement physical, electronic, and managerial policies, procedures, and safeguards to prevent unauthorized access, use, or disclosure of Personal Information.

The Vendor shall make the Personal Information available to amend as directed by the City and

incorporate any amendments into all the copies maintained by the Vendor or its subcontractors and agents. Vendor shall certify its destruction after ninety (90) calendar days and the Vendor shall retain no copies. If Vendor and City mutually determine that return or destruction is not feasible, the Vendor shall not use the Personal Information in a manner other than those permitted or authorized by state and federal laws.

The Vendor shall notify the City in writing within 96 hours upon becoming aware of any unauthorized access, use, or disclosure of Personal Information. Vendor shall take necessary steps to mitigate any harmful effects of such use or disclosure. Vendor is financially responsible for notification of any unauthorized access, use or disclosure. The details of the notification must be approved by the City. Any breach of this clause may result in immediate termination of the Agreement by the City and the demand for return of all Personal Information.

Vendor agrees that prior to the Effective Date of this Agreement, Vendor will, at its expense, conduct or have conducted within the last 12 months, the following, and thereafter, Vendor will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Compromise:

- A PCI, SOC 2 or other mutually agreed upon audit of Vendor's security policies, procedures and controls;
- A vulnerability scan, performed by a Third Party scanner, of Vendor's systems and facilities that are used in any way to deliver services under this Agreement; and,
- A formal penetration test, performed by a process and qualified personnel, of Contractor's systems and facilities that are used in any way to deliver services under this Agreement.

The same will be evidenced by providing the City a copy of the Successful Audit Letter and a Scope of Audit Document (outlining what is included in the audit). Audit Report will not include "private" information, defined as proprietary environment/infrastructure detail not specific to systems that process or transmit City Data.

Vendor to comply with PII (Personally Identifiable Information) or SPI (Sensitive Personal Information) by signing **Appendix B** 'IT Cloud Vendor Security Agreement' agreeing to follow security best practices.

Section 8 CONFIDENTIALITY

Neither party will disclose the other party's or its affiliates' confidential or proprietary information, including Transaction Data and User Profile Data ("Confidential Information") (including the terms of this Agreement and any information provided by the other party that is confidentially maintained or proprietary or which derives value from not being generally known to persons who can obtain economic value from its disclosure or use or that a reasonable person would consider confidential, given the context) except:

- i) with the other party's consent;
- ii) to employees, agents and contractors who have a need to know in the discharge of their duties and who are subject to a contractual obligation to keep such information confidential that is at least as restrictive as this Agreement; or
- iii) when required to do so by law or by any binding rule, order or request.

For purposes of this Section 8, the parties agree that confidential or proprietary information does not include any information that is:

- i) already known to the receiving party at the time of disclosure hereunder (other than from the other party or its affiliates) as demonstrated by its written records;
- ii) now or hereafter becomes publicly known other than through acts or omissions of the receiving party, or anyone to whom the receiving party disclosed such information;

- iii) disclosed to the receiving party, by a third party, under no obligation of confidentiality to the disclosing party or any other party; or
- iv) independently developed by the receiving party without reliance on the confidential information of the disclosing party as shown by its written records.

Each party shall exercise reasonable commercial care in protecting the confidentiality of the other party's confidential information disclosed to it. The parties agree that an actual or threatened breach of this provision would result in irreparable harm to the party whose confidential information would be disclosed in breach, and shall entitle that party to temporary or permanent injunctive relief without proof of actual damages.

Section 9 MISCELLANEOUS

9.1 ASSIGNMENT

This Agreement shall be binding on the parties, their successors and their permitted assigns. PayByPhone may assign its rights or obligations under this Agreement without Client consent.

9.2 AMENDMENT

All amendments to this Agreement shall be in writing. In the event Client wishes to add new Parking Locations in addition to the Initial Parking Locations (the "Additional Parking Locations") or to add parking spaces to an existing Parking Location, the amendment will be effective against both parties if it is in the form of email between implementation personnel of the parties and, effective the date of such email, the Appendix A will be read to include these Additional Parking Locations or parking spaces.

9.3 SURVIVAL

The confidentiality, intellectual property and indemnification obligations in this Agreement and any other terms that by reasonable implication contemplate continued performance, shall survive the expiry or termination of this Agreement.

9.4 NO AGENCY

Each party, in all matters relating to this Agreement, will act as an independent contractor and independent employers. Except as otherwise expressly set forth herein, neither party will have authority and will not represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other, or to represent the other as an agent, employee or in any other capacity. Except as otherwise expressly set forth herein, nothing in this Agreement shall be construed to have established any agency, joint venture or partnership between the parties. Neither party shall make any warranties or representations on behalf of the other party.

9.5 GOVERNING LAW

This Agreement, and all matters relating hereto, shall be governed in all respects by the laws of the State of Washington, excluding the application of any conflict of laws principles and/or rules. The parties hereby agree that all disputes arising out of this Agreement shall be subject to the exclusive jurisdiction of and venue in the competent courts located in State of Washington, and consent to the personal and exclusive jurisdiction and venue of these courts.

9.6 SEVERABILITY

In the event that any provision of this Agreement shall be unenforceable or invalid under any applicable law or be so held by applicable court decision, such unenforceability or invalidity shall not render this Agreement unenforceable or invalid as a whole, and, in such event, such provision shall be changed and interpreted so as to best accomplish the objectives of such unenforceable or invalid provision within the limits of applicable law or applicable court decisions.

9.7 ATTORNEY'S FEES

In any legal proceeding between the parties, the prevailing party shall be entitled to recover reasonable attorney's fees and expenses.

9.8 FORCE MAJEURE

If performance hereunder is prevented, restricted or interfered with by any act or condition whatsoever beyond the reasonable control of a party, the party so affected, upon giving prompt notice to the other party, shall be excused from such performance to the extent of such prevention, restriction or interference.

9.9 ENTIRE AGREEMENT

This Agreement, together with the appendices attached to it, constitutes the entire agreement between the parties with respect to the subject matter hereof. This Agreement supersedes, and the terms of this Agreement govern, any prior agreements with respect to the subject matter hereof. This Agreement may not be modified, amended or any provision waived except by the parties' mutual written agreement.

9.10 NO WAIVER

Failure by either party to enforce any provision of this Agreement (whether in any one or more instance) shall not be deemed a waiver of future enforcement of that or any other provision.

9.11 NOTICE

Any notices provided hereunder shall be given at the address of the recipient specified below or at such other address as specified in writing. Any notice or other communication required to be given hereunder by either party shall be deemed duly given (a) when personally delivered to the other party, or (b) on the date of receipt when such notice was mailed by certified mail, postage prepaid and return receipt requested, addressed to the other party at the address set forth above, or such other address as either party may designate by giving written notice to the other; or (c) on the date of receipt when such notice was sent by facsimile or e-mail to the other party; provided the sending party receives a written or electronic notice of receipt from the other party of the facsimile or e-mail.

9.12 COUNTERPARTS

This Agreement may be executed in one or more counterparts, each of which shall be deemed an original and all of which shall be taken together and deemed to be one instrument. The parties further agree that a signature transmitted via facsimile shall be deemed original for all purposes hereunder.

9.13 CAPTIONS

The captions used in this Agreement are for convenience only and shall not affect in any way the meaning or interpretation of the provision set forth herein.

9.14 AGREEMENT APPROVAL

Each party hereby represents and warrants that all necessary corporate and/or governmental approvals for this Agreement have been obtained, and the person whose signature appears below has the authority necessary to execute this Agreement on behalf of the party indicated.

9.15 SOPHISTICATION OF PARTIES

Each party to this Agreement represents that it is a sophisticated commercial party capable of understanding all of the terms of this Agreement, that it has had an opportunity to review this Agreement with its counsel, and that it enters this Agreement with full knowledge of the terms of the agreement.

9.16 CLIENT'S CONDUCT OF BUSINESS THROUGH AFFILIATES

The parties acknowledge that Client may carry out its business through affiliates. Client agrees to cause its affiliates to take such actions and to execute such documents as may be reasonably required to give effect to this Agreement as though references to Client in this Agreement were references to Client and those of its affiliates through which it carries on the business of owning and operating parking facilities.

9.17 PCI-DSS: PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

PayByPhone is responsible for the security of cardholder data which PayByPhone possesses or otherwise stores, processes, or transmits on behalf of the Client. PayByPhone abides by the rules and regulations set forth in the PCI-DSS.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives.

City of Kirkland

PayByPhone US Inc.

Signature: *Julie Underwood*
Julie Underwood (Apr 5, 2024 15:59 PDT)

Signature: *Teresa Trussell*
Teresa Trussell (Apr 4, 2024 11:21 EDT)

Name: Julie Underwood

Name: Teresa Trussell

Title: Deputy City Manager of Operations

Title: President

Notice Address:
123 Fifth Ave.
Kirkland, WA.
98033, US

Notice Address:
c/o PayByPhone Technologies Inc.
600-1290 Homer Street, 6th Floor
Vancouver, BC V6B 2Y5 Canada
With a copy to: legal@paybyphone.com

APPENDIX A

PARKING FACILITIES AND METERED PARKING STALLS:

Parking facility located at Lake & Central Lot including 54 of parking spaces.

Parking facility located at Lakeshore Lot including 131 of parking spaces.

(together, “Initial Parking Locations”).

PRICING:

All amounts are exclusive of any and all taxes, including taxes applicable on fees paid by driver.

For the purposes of this Agreement “Transaction” includes (a) user registration for a parking session, permit, validation or extension at a Parking Location through the PayByPhone mobile payment service (whether or not any amount is payable to Client by the user), (b) a refund, (c) a charge reversal and (d) any other operation for which PayByPhone incurs a fee from its gateway provider or an acquirer, if applicable.

ITEM	PRICE
ONE-TIME SETUP FEES	
Signage – first round of signage production at service launch (installation not included)	Included
Training, consulting, marketing, and customer support as described in the Agreement	Included
Mobile payment services setup fee for all Initial Parking Locations	\$0.00 ¹
Integration with enforcement solution software	TBD
Standard PayByPhone city dynamic label	Included
TRANSACTION FEES	
Client pays to PayByPhone per Transaction (Client may charge driver a non-embedded, on-top of price of parking convenience fee of \$0.40)	\$0.40 ²
Monthly minimum of total Transaction Fees	\$150/mo. ³
OPTIONAL FEES	
Custom dynamic label	\$1,000
Mobile payment service setup fee for Additional Parking Locations	\$250 per location

NOTES:

1. Mobile payment services setup fee includes configuration, testing and implementation of a dedicated client account within the PayByPhone system; merchant account integration and testing; set up and training on reporting, customer service and other elements of the PayByPhone Service Management Interface. One-time setup fees are invoiced at contract signing.
2. Any change in the convenience fee will not affect the price the Client will pay to PayByPhone per Transaction. The convenience fee may only be increased by mutual agreement of both parties. Services covered by the Transaction Fee includes interactive voice response solution (IVR).
3. Monthly minimum will apply when Transaction Fees per calendar month total less than the specified monthly minimum. Client is responsible for covering the difference between the monthly minimum and the Transaction Fees.

4. Client is responsible for paying all Transactions Fees and any IVR additional per transaction fees for all Transactions made through the PayByPhone mobile application, web application, and/or IVR (if applicable).
5. Client is responsible for paying its own credit card processing and merchant banking fees, if Client is MOR.
6. In the event that PayByPhone is the only form of payment, Client will be responsible for 100% of the call centre fees as a pass through.
7. All fees and charges are payable within 30 days of invoicing.

APPENDIX B

IT Cloud Vendor Security Agreement

This IT Cloud Vendor Security Agreement (“Security Agreement”) is entered into by and between the City of Kirkland, (“City”), and _____ (“Vendor”).

Scope: This policy applies to all Vendors who do any form of work (“Contract”) with the City of Kirkland that includes possession, storage, processing, or transmission of Personally Identifiable Information (PII), Sensitive Personal Information (SPI) or Personal Health Information (PHI) for City of Kirkland employees, volunteers, contractors, and/or citizens in any location that is outside of the City of Kirkland Firewalls. This includes public and private cloud infrastructures and Vendor’s own infrastructure on their premises. This is regardless of who the Vendor is and which department they are working for or with, and it applies to all locations where the Vendor stores information.

If this Contract covers only PII or SPI, then only this addendum must be signed.

If this Contract covers PHI, then this addendum must be signed, and a HIPAA Business Associates Agreement must also be signed and incorporated as an addendum to this document or as an addendum to the Contract.

This policy does NOT apply to CJIS data (criminal justice data). There is a separate federally mandated addendum that covers protection of CJIS data, which must also be signed if the Contract includes such information.

Provision: When possible, this policy should be an addendum to existing contracts with vendors. It may be signed separately when necessary.

Duration: This policy applies from the time a vendor signs its Contract with the City through such point in time that all data which was in the vendor’s control is returned to the City and destroyed at the City’s request, including but not limited to backups, test sites, and disaster recovery sites.

Definitions:

Personally Identifiable Information (PII), or Sensitive Personal Information (SPI): Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Protected Health Information (PHI): any information about health status, provision of health care, or payment for health care that can be linked to a specific individual, which is more particularly defined under HIPAA (Title 45, CFR) and the Health Care Information Act (RCW Chapter 70.02).

Vendor: Includes owners and employees, volunteers, subsidiaries, and any subcontractors who might reasonably have access to this data.

Options:

Option 1: A vendor can verify that they have a high level of security certification that is satisfactory to the City of Kirkland. Examples include but may not be limited to SOC2 and FedRamp.

If this option is selected, print the mutually agreed upon certification level below and attach appropriate documentation.

Option 2: Vendors can agree to follow the following security best practices:

1. All customer data will be stored on servers physically located in the United States or Canada.
2. All customer data will be stored in a location with reasonable physical controls where data will not be visible to anyone not covered by this policy.
3. Access to data will only be provided on a need to know basis in order for the vendor to complete this work.
4. Data will not be shared with an outside third party without explicit written consent of the City.
5. Data will be encrypted prior to and during any transfer from one location to another.
6. Data will be disposed of appropriately, including shredding or burning of any printed versions and destruction or secure erasure of any electronic medium on which data has been stored.
7. Vendor agrees to the appropriate internal certification for vendor staff who access the data (for example, PHI must only be handled by vendors who have HIPPA training).
8. Vendor staff with access to City of Kirkland data covered by this policy must pass a criminal background check prior to accessing that data.
9. Vendors must perform internal and/or external security auditing on a regular basis that is no less common than once per year.
10. Vendors shall abide by the following policies for passwords:
 - a. Network login passwords must be at least 8 characters long and include at least one number and one capital letter.
 - b. Passwords must be changed every 90 days.
 - c. The same password cannot be re-used within twenty password changes.
 - d. Passwords must not be written down or stored in systems except in encrypted applications designed to store passwords.
 - e. Passwords must not be shared among vendor staff.
 - f. Vendors should not use the same passwords for City and personal needs.
 - g. Other password protected systems will comply with above network login password policy when technically possible.
11. Vendors must report all security incidents to the appropriate City of Kirkland IT personnel, including any serious security breaches on their own network, within 96 hours of identifying the security incident.
12. In the event of a data breach, Vendor must have an internal policy to provide for timely forensic investigation of affected and related servers and must follow all state, local, and federal requirements for notifying individual's whose PII or PHI has been or may have been breached.
13. Vendor's servers must be patched on a regular and timely basis with all security-related patches from application and infrastructure vendors.
14. Data must be kept in at least two different physical locations. One location can be in a compressed format (e.g., as a backup file).
15. Vendor must enable logging as follows:
 - a. Logs are enabled for common third-party applications
 - b. Logs are active by default
 - c. Logs are available for review by the City of Kirkland for up to one year
 - d. Logs are retained for up to one year

Any deviation from the above best practices must be described here and mutually agreed upon (Signatures on this policy will constitute mutual agreement).

Description of any area where vendor is requesting a waiver, an agreement to a different method, or any other change to this policy:

A breach of this Security Agreement also constitutes a breach of any agreement to which it is appended and the City may terminate either or both because of such breach as soon as it must to mitigate that breach or others that may then be apparently forthcoming. The City agrees to work with the Vendor to avoid such termination if reasonably possible but protection of the information held by the Vendor cannot be compromised in the process.

Description of data in the Vendor's care (attach additional sheets if necessary): See section 4.2 and 4.3 of the Agreement

Is this an addendum to an existing or new contract (Y/N): Y

If yes, name and duration of contract: Cooperation and Service Agreement. 3-year duration with option to renew for one or more additional terms of one year.

City business person responsible for contract and vendor management:

Name	Title	Department
------	-------	------------

City IT person responsible for contract and vendor management:

Name	Title	Department
------	-------	------------

The following signature block must be completed. By signing this agreement, vendor warrants that they are responsible for the security of the PII, SPI, and/or PHI in their care.

VENDOR NAME
<u><i>Teresa Trussell</i></u> <small>Teresa Trussell (Apr 4, 2024 11:21 EDT)</small>
Signature
Teresa Trussell
Printed Name
President
Title
Apr 4, 2024
Date

City of Kirkland
<u><i>Mary Jensen</i></u>
Signature
Mary Jensen
Printed Name
IT Manager - Enterprise Applications and GIS
Title
Apr 4, 2024
Date



PayByPhone Technologies, Inc.

Type II System and Organization Controls Report (SOC 2)

Report on a Service Organization's Description of Its System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, Processing Integrity, and Confidentiality Throughout the Period November 1, 2022, to October 31, 2023.



KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

KirkpatrickPrice.

innovation. integrity. delivered.

TABLE OF CONTENTS

SECTION I: ASSERTION OF PAYBYPHONE TECHNOLOGIES, INC. MANAGEMENT	1
Assertion of PayByPhone Technologies, Inc. Management.....	2
SECTION II: INDEPENDENT SERVICE AUDITOR’S REPORT	4
Independent Service Auditor’s Report	5
Scope	5
Service Organization’s Responsibilities	6
Service Auditor’s Responsibilities	6
Inherent Limitations	7
Description of Tests of Controls.....	7
Opinion	7
Restricted Use.....	8
SECTION III: PAYBYPHONE TECHNOLOGIES, INC.’S DESCRIPTION OF ITS PAYMENT PROCESSING SERVICES SYSTEM.....	9
Services Provided	10
Principal Service Commitments and System Requirements.....	12
Regulatory Commitments	12
Contractual Commitments.....	12
System Design.....	12
Components of the System Used to Provide the Services	13
Infrastructure	13
Software	13
People.....	13
Data	14
Processes and Procedures.....	15
Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring	16
Control Environment.....	16
Management Philosophy.....	16
Security, Availability, Confidentiality, and Processing Integrity Management	17
Security, Availability, Confidentiality, and Processing Integrity Policies.....	17
Personnel Security	17
Physical Security and Environmental Controls	19
Change Management	19
Application Development	20

Application Change Management	21
System Monitoring	21
Problem Management	23
Data Backup and Recovery.....	23
System Account Management	24
Risk Assessment Process	26
Information and Communication Systems	26
Vendor Management.....	27
Monitoring Controls.....	27
Changes to the System During the Period.....	28
Complementary User-Entity Controls	29
SECTION IV: TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS	31
Applicable Trust Services Criteria Relevant to Security, Availability, Confidentiality, and Processing Integrity	32
Security	32
Availability.....	32
Processing Integrity.....	32
Confidentiality.....	33
Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories.....	34
Control Environment	34
Communication and Information.....	42
Risk Assessment	47
Monitoring Activities.....	52
Control Activities.....	54
Logical and Physical Access Controls.....	58
System Operations.....	75
Change Management	86
Risk Mitigation.....	92
Additional Criteria for Availability.....	95
Additional Criteria for Confidentiality.....	100
Additional Criteria for Processing Integrity.....	102

**SECTION I:
ASSERTION OF PAYBYPHONE TECHNOLOGIES, INC.
MANAGEMENT**

ASSERTION OF PAYBYPHONE TECHNOLOGIES, INC. MANAGEMENT

We have prepared the accompanying description in section III titled “PayByPhone Technologies, Inc.’s Description of Its Payment Processing Services System” throughout the period November 1, 2022, to October 31, 2023, (description), based on the criteria for a description of a service organization’s system in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report (AICPA, Description Criteria)*, (description criteria). The description is intended to provide report users with information about the payment processing services system that may be useful when assessing the risks arising from interactions with PayByPhone Technologies, Inc.’s system, particularly information about system controls that PayByPhone Technologies, Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and processing integrity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

PayByPhone Technologies, Inc. uses Amazon Web Services (AWS) for cloud infrastructure services, Network Merchants for payment gateway platform services, Accertify for payment gateway platform services, Worldline (fka Ingenico eCommerce Solutions/Ogone) for payment solution services, Valtix for cloud security services, Apigee for full lifecycle application programming interface (API) management services, and Twilio for interactive voice response (IVR) systems services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PayByPhone Technologies, Inc., to achieve PayByPhone Technologies, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents PayByPhone Technologies, Inc.’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of PayByPhone Technologies, Inc.’s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at PayByPhone Technologies, Inc., to achieve PayByPhone Technologies, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents PayByPhone Technologies, Inc.’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of PayByPhone Technologies, Inc.’s controls.

We confirm, to the best of our knowledge and belief, that

- a. the description presents PayByPhone Technologies, Inc.’s payment processing services system that was designed and implemented throughout the period November 1, 2022, to October 31, 2023, in accordance with the description criteria.

- b. the controls stated in the description were suitably designed throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of PayByPhone Technologies, Inc.'s controls throughout that period.

- c. the controls stated in the description operated effectively throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of PayByPhone Technologies, Inc.'s controls operated effectively throughout that period.

SECTION II: INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Jonny Combe
President and CEO
PayByPhone Technologies, Inc.
600-1290 Homer Street, 6th Floor
Vancouver, BC
V6B 2Y5, Canada

Scope

We have examined PayByPhone Technologies, Inc.'s accompanying description in section III titled "PayByPhone Technologies, Inc.'s Description of Its Payment Processing Services System" throughout the period November 1, 2022, to October 31, 2023, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and processing integrity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

PayByPhone Technologies, Inc. uses AWS for cloud infrastructure services, Network Merchants for payment gateway platform services, Accertify for payment gateway platform services, Worldline (fka Ingenico eCommerce Solutions/Ogone) for payment solution services, Valtix for cloud security services, Apigee for full lifecycle API management services, and Twilio for IVR systems services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PayByPhone Technologies, Inc., to achieve PayByPhone Technologies, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents PayByPhone Technologies, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of PayByPhone Technologies, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at PayByPhone Technologies, Inc., to achieve PayByPhone Technologies, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents PayByPhone Technologies, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of PayByPhone Technologies, Inc.'s controls. Our examination did not include such

complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

PayByPhone Technologies, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements were achieved. In section I, PayByPhone Technologies, Inc. has provided its assertion titled "Assertion of PayByPhone Technologies, Inc. Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. PayByPhone Technologies, Inc. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

- a. the description presents PayByPhone Technologies, Inc.'s payment processing services system that was designed and implemented throughout the period November 1, 2022, to October 31, 2023, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of PayByPhone Technologies, Inc.'s controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls

and complementary user entity controls assumed in the design of PayByPhone Technologies, Inc.'s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of PayByPhone Technologies, Inc., user entities of PayByPhone Technologies, Inc.'s payment processing services system during some or all of the period November 1, 2022, to October 31, 2023, business partners of PayByPhone Technologies, Inc. subject to risks arising from interactions with the payment processing services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

January 16, 2024

SECTION III: PAYBYPHONE TECHNOLOGIES, INC.'S DESCRIPTION OF ITS PAYMENT PROCESSING SERVICES SYSTEM

SERVICES PROVIDED

PayByPhone Technologies, Inc. (PayByPhone) functions as both a business-to-business and business-to-business-to-consumer organization. Business-to-business-to-consumer operations allow PayByPhone consumers to pay for on-street or off-street parking with their phone without using a parking meter. The service allows motorists with several different options and features, including the following:

- A SMS reminder before a parking session expires
- Ability to extend parking sessions remotely
- Transaction reporting
- Email parking receipts
- Parking authority notifications

The business-to-business operations allows parking operators to increasingly recognize that mobile payments can both reduce the costs associated with operating expensive pay and display machines as well as increasing revenue per parking session. In addition to lowering operational costs, PayByPhone also provides detailed analytics and professional services for the parking industry.

Client Sales and Onboarding

Internal sales personnel respond to requests for proposal (RFPs) and other sales leads to identify cities, counties, or government entities and individual parking companies that could potentially use PayByPhone services. Once a contract is signed, a project manager, implementation manager, and occasionally a client success member is assigned to the project. Onboarding is tracked through Google Sheets or Microsoft Excel spreadsheets and corresponding checklists. Suppliers are engaged to produce parking signs.

Using an emailed Excel spreadsheet, PayByPhone collects information related to the locations and parking spaces covered in the services, pricing, portal users and permissions, and financial details to facilitate payment collection and disbursements. The implementation manager uses the information to setup an account in the PayByPhone Backoffice application using all the provided details. A portal training session is provided to introduce client personnel to the portal and to demonstrate all of the features for the client's locations. Testing is performed with the client to validate proper configurations. Immediately following the go-live event, clients are transitioned to the Client Success Account Manager team for long-term support.

Clients use the Backoffice application to generate activity-related reports such as space and lot usage and monthly revenues related to the city or business. As needed, ongoing client support is provided the Client Success Account Manager.

Ongoing Transaction Processing and Support

Once live, parking users can use cell phones to connect to the IVR system or cell phone. Users can also use web-based applications to connect to the online system to make payments. Cardholder data (CHD) and personally identifiable data (PII) is transmitted from the cell phone and web-based

application frontends to an application programming interface (API) over Transport Layer Security (TLS) v1.2 for processing and storage. Data can also be received via Twilio's IVR service, which connects to Apigee API platform and forwards PayByPhone-specific traffic. Apigee forwards the data over a mutually authenticated TLS (mTLS) session to an AWS web application firewall (WAF), where the traffic is decrypted on the Nginx system. The data is then re-encrypted and sent via HTTPS or TLS over virtual private cloud (VPC), where it is decrypted and passed to AWS Lambda functions. AWS Lambda is the interface point between Twilio IVR systems and PayByPhone's IVR systems in the eStructure data center. AWS Lambda makes an API call over TLS 1.2 and routed through AWS Transit Gateway and Valtix Gateway Hub to the load balancer or API, which resides at the eStructure data center.

Additionally, channels are in place in order for consumers to engage PayByPhone for support. The Yoummday (fka ICON) third party provides Zendesk-driven support to consumers. The vendor works incoming Zendesk tickets and resolves issues as they are able. Tier 2 support is escalated to an internal team within PayByPhone, and Tier 3 support is escalated to the Development team using a Jira ticket.

Client Offboarding

Offboarding starts once a client has provided notification that the relationship is to be terminated. A departure date is set, and on that date, the project manager stops the services and merchant accounts in Backoffice. Clients continue to have access to Backoffice to generate reports for 30 days, or longer if agreed on at the termination notification. Once this date has passed, the project manager removes all access for the client in Backoffice.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

The organization adheres to regulatory measures that impact its operations. The Data Protection Policy establishes data governance practices that define the organization's process of managing the availability, usability, integrity, and security of the data in enterprise systems in accordance with all legal, regulatory, compliance, and business requirements. PayByPhone adheres to the following business and regulatory compliance requirements:

- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- Canadian Consumer Privacy Protection Act (CPPA)
- European Union General Data Protection Regulation (GDPR)
- Payment Card Industry Digital Security Standards (PCI DSS)
- California Consumer Privacy Act (CCPA)

Contractual Commitments

Contractual materials are used to communicate descriptions of services to the organization's clients. The descriptions of services and responsibilities are documented in contracts, which must be established before services are provided. The contracts include the following:

- Intellectual property rights
- Definition of and responsibilities pertaining to "client data"
- Definition of and responsibilities pertaining to "Customer" (parker) data
- Mutual indemnification
- Mutual confidentiality and non-disclosure
- Survival of specific clauses in the event of contract termination (specifically, confidentiality, intellectual property and indemnification clauses)
- PayByPhone responsibility to maintain PCI DSS compliance

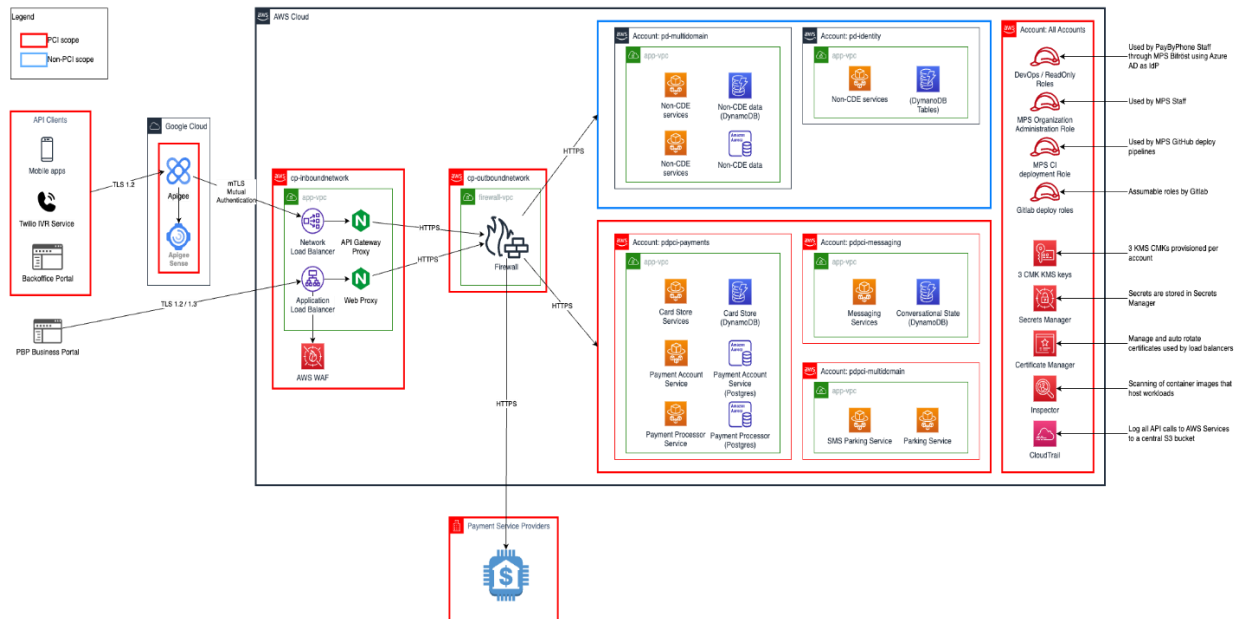
System Design

PayByPhone designs its payment processing services system to meet its regulatory and contractual commitments. These commitments are based on the services that PayByPhone provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that PayByPhone has established for its services. PayByPhone establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in PayByPhone's system policies and procedures, system design documentation, and contracts with clients.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

Infrastructure

PayByPhone maintains formally documented network diagrams that illustrate the infrastructure for both the PCI and corporate networks. The diagrams must be reviewed annually and updated after changes to the networks. The high-level network topology diagram is shown below. The organization also maintains a system inventory that captures the device name, device type, vendor, function, OS, location, and additional notes.



Rev	DATE	DESCRIPTION	By
1	2023-08-09	New Diagram to reflect AWS & Cloud native infrastructure	JD Stuart

Software

PayByPhone maintains a software inventory for all business and critical software in use within the environment. The critical software in use includes the following:

- Alpine Linux
- Windows Server 2019
- Amazon Cloud Firewall
- Nginx
- Ubuntu

People

A management board (M-Board) is established to provide oversight and direction to the organization. The PayByPhone M-Board consists of the PayByPhone Chief Executive Officer

(CEO), Chief Technology Officer (CTO), and Chief Financial Officer (CFO). During monthly M-Board meetings, compliance and information security topics are covered.

The company senior leadership consists of the CEO, CFO, and CTO, who are responsible for all day-to-day operations. Security and IT Compliance reports through the CTO organization as one of three permanent PayByPhone board members. A process is in place to ensure that certain activities, such as decisions and transaction choices, must be approved by at least two people. The organization chart illustrates the separation of duties, company structure, and reporting lines.

Data

PayByPhone has a standardized process in place for handling cardholder data and data related to the application service offerings. PayByPhone receives, stores, and/or transmits personal account numbers (PANs), CVV, expiry, username, email address, communication preference, (occasionally) picture of car, geolocation, license plate and region, zip code, name, account password, and vehicle description into PayByPhone systems. PayByPhone stores, transmits, and processes the full PAN and expiration date for all major card schemes; however, the CVV is never stored past the authorization step of the transaction.

Sensitive data is secured any time it must be transmitted or received via open, public networks. Cryptography configurations for APIs and application require that only traffic on TLS ports (TCP/443) is received in communication between all system components. TLS 1.2 other and strong cipher suite selections are supported, including the following:

- Key exchanges supporting perfect forward secrecy with key lengths of 2048+ (FFC) and 256+ (elliptic curve)
- RSA host authentication with key lengths of 2048+
- AES128, AES256 and ChaCha20 bulk encryption SHA256 or stronger MAC

Data is also encryption when at rest. Encryption of PII is accomplished through AWS RDS-based encryption using an encryption key managed in AWS Key Management Service (KMS). Encryption of CHD is performed by the Backoffice application using a custom-built application component that uses AWS-provided software development kits (SDKs) to interface with AWS KMS, and each data element is encrypted its own KMS-managed encryption key and stored in the database as encrypted content. AWS Guardrails is used to encrypt all databases.

The organization uses AWS to manage encryption keys. In AWS KMS, key-encrypting keys are automatically rotated on an annual basis, and encryption keys are retained in an isolated AWS account to provide additional access control for team members that can interact with the KMS. Additionally, access to encryption keys is managed by submitting a ticket to the Security and Compliance Service Desk.

Data is classified into one of three defined categories: sensitive, private, and public. Sensitive data applies to less sensitive business information, which is intended for use within PayByPhone; unauthorized disclosure could adversely impact the company, its stockholders, its business partners, and/or its customers. Private data applies to personal information, which is intended for use within PayByPhone; unauthorized disclosure could adversely impact the company and/or its

employees. Public data applies to all other information that does not fit into the aforementioned categories; unauthorized disclosure is not expected to seriously or adversely impact the company.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

The security, availability, confidentiality, and processing integrity categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security, availability, confidentiality, and processing integrity criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security, availability, confidentiality, and processing integrity criteria are included in section IV of this report. Although the applicable trust services criteria and related controls are included in section IV, they are an integral part of PayByPhone's description of its payment processing services system.

Control Environment

Management Philosophy

The organization relies on leadership and conducts training to ensure that security and compliance are prioritized. Leadership's primary objective is to ensure compliance, which is obtained through educating and communicating with employees. The compliance program is enforced through a quarterly presentation between the Compliance team and leadership to cover the top five initiatives. All compliance efforts are communicated to the PayByPhone Product Steering Board (PSB) to ensure that the compliance program contributes to corporate values. The core values of the company are:

- See through customers' eyes
- Work together
- Stay curious
- Have fun
- Make things happen

Corporate policies and company handbooks are used to communicate guidelines and company expectations, and these policies and handbooks are continuously available for review in Confluence. The Global Guidelines capture guidelines related to crisis communication, analyzing and reporting a data breach to the authorities and data subjects, data subject requests, and compliance requirements. The Global Policies document captures top-level principles and policies on specific subject matter, including a Data Protection Policy, Data Retention Policy, Global Information Security Policies, Security Incident Response Policy, and Background Check Policy. The North American Organizational Handbook addresses the following North American policies and guidelines:

- Remote Work Health & Safety Policy
- Sick & Personal Time Off Policy
- Time Off Vacation Policy
- Equal Employment Opportunity Policy

A Code of Conduct is maintained that communicates company values as well as ethical and behavioral expectations to employees. The Code of Conduct includes the following:

- Messages regarding integrity and compliance
- Social responsibility
- Responsibilities to business partners
- Commitments to other teammates
- Occupational safety and healthcare
- Data protection
- Security and protection of information
- Know-how and intellectual property
- IT security
- Handling company assets

Leadership maintains continuous communication with employees, including meetings and emails, to ensure employees are aware of the tone and direction of the company. The organization conducts monthly business update meetings, conducts weekly all-hands meeting, distributes weekly development and product news emails, and holds development and product quarterly townhall meetings. Quarterly leadership reviews are completed with the management board (CEO, CTO, and CFO), and weekly one-on-one meetings are held between Compliance and the Chief Information Security Officer (CISO) & Senior Director of Reliability.

Security, Availability, Confidentiality, and Processing Integrity Management

The organization's security, availability, confidentiality, and processing integrity requirements are managed using a combination of documented policies and procedures, management oversight, and network systems and hardware. These management practices are implemented in all areas of the control environment to protect systems, data, and personnel and to ensure compliance with industry best practices and standards.

Security, Availability, Confidentiality, and Processing Integrity Policies

The organization has a process for continuously reviewing and updating the Information Security Policies and Procedures. The Security team is responsible for creating and updating policies, and management is responsible for approving the policy. The Information Security Policies and Procedures is a monolithic information security policy that includes an internal review and approval. As a Jira-based document, Information Security Policies and Procedures is continuously updated as needed. The CTO, or their designee, is responsible for managing the information security policy. The Information Security Policies and Procedures are reviewed annually by the M-Board before incorporating it into the Global Organization Handbook. Confluence is used to distribute information security policies to all parties.

Personnel Security

PayByPhone maintains a process for hiring and onboarding new employees. The organization maintains formally documented job descriptions for personnel. Within the job descriptions, information security concerns are captured, and the job descriptions are considered when recruiting and hiring new employees. All potential employees and contractors undergo a Sterling

background check before being hired. Background checks are completed in accordance with all local laws and regulations and includes the following:

- Verification of name, address, and date of birth
- Verification of official identification and Social Security number
- Verification of employment and educational records
- Review of credit checks, federal or state criminal record checks, and reference checks
- Conduct drug screenings as applicable and allowed by law

After an employee passes the background check, onboarding activities are completed. The onboarding activities are outlined in the Employee Onboarding Checklist and managed in BambooHR to ensure all employees are consistently onboarded. Managers are responsible for preparing an onboarding plan, forwarding recurring calendar invites and inviting the new team member to appropriate Slack channels, and communicating the laptop requirements to the talent acquisition partner. The employee's tasks in the onboarding process involve reviewing the health and safety information, reviewing the organizational handbook and code of conduct, reviewing the day one orientation files and bookmarking links, and reviewing and signing the company policies. During onboarding, new hires complete tax forms, eligibility forms, payroll forms, bank deposits, protection of corporate interests' agreement, technology onboarding, and confidentiality agreement. Additionally, all new employees must attend and acknowledge completion of the organization's Security Program, which addresses the following:

- Awareness training
- Risk assessment
- Policies and procedures
- Business case studies
- What is a Security Incident?
- Examples of non-public private information (NPPI)
- Indications of an attack (security event)
- Examples of confidentiality, integrity, and availability incidents
- How to respond to when a security incident is detected

Training and continuous education opportunities are provided to employees via the Inspired eLearning learning management system (LMS). General security awareness training is provided through the Inspired eLearning LMS, and new campaigns are run quarterly to keep training fresh and short for all users. All new hires are provided security awareness training on a bi-monthly schedule where the session is conducted either in-person or through web conference, as appropriate. Additionally, the LMS captures each user's acknowledgement of their receipt and understanding of the Information Security Policy.

Performance evaluations and reviews are completed on a regular basis to ensure expectations are being met. Ongoing one-on-ones with managers are completed on a frequency established by the employee and manager, and coaching between employees and leadership is completed when performance expectations are not being met. Salary reviews are performed annually.

PayByPhone has a process in place that considers voluntary and involuntary terminations. In the event of voluntary termination, the employees must provide a 30-day notice, as stipulated in the Employment Agreement, but the organization attempts to accommodate shorter if needed. The

termination process begins in BambooHR and requires submitting a “Joiners and Leavers” ticket in Jira to manage the process with all parties. In the event of involuntary termination, a similar process is followed, but with greater urgency in coordination between all the parties. In both cases, equipment is returned through a courier service and compared against IT asset inventory. The termination process is managed in BambooHR and Jira tickets.

Physical Security and Environmental Controls

Although physical security safeguards are implemented in office locations and there are employees who access in-scope data from the offices, these locations do not provide any special access to PII or to critical applications and are considered out of scope for this assessment. All critical systems and applications are located in AWS. Physical and environmental security of the PayByPhone data housed in AWS is the responsibility of AWS. Interested parties should review the AWS audit report.

PayByPhone implements mobile device management (MDM) processes to ensure that remote users have their devices protected. All company end-user devices are required to use desktop firewalls and connect using Zero Trust Network Access (ZTNA) solutions provided by the company. The Mobile Device Management Policy requires the use of personal firewalls and use of the Zscaler Zero Trust Network Access solution for remote access to company applications. All end-user devices are managed through MDM platforms: Windows devices use Microsoft Intune, and MacOS devices use Mosyle Enhanced Apple Device Management.

The organization has a process for destroying and disposing of data and media when no longer needed. In accordance with the Disposal Policy, all electronic and hardcopy data, when no longer needed for legal, regulatory, or business requirements, must be securely deleted from PayByPhone systems. Before computer or communications equipment can be sent to a vendor for trade-in, servicing or disposal, all cardholder data must be destroyed or removed according to the approved methods. Outsourced destruction of media containing cardholder data must use a disposal vendor that provides a Certificate of Destruction. Media that can be re-used must have the data securely deleted and wiped using a utility approved by the Systems Group. PayByPhone has the following requirements in place for destroying media:

- Hard disks are sanitized using a National Institute of Standards and Technology (NIST) 800-88 standard degauss or crosscut shred to, or by penetrating the disk platters with one or more half inch holes drilled through them
- Floppy disks are disintegrated, incinerated, pulverized, crosscut shred, or melted
- Tape media are degaussed, crosscut shred, incinerated, pulverized, or melted
- USB thumb drives, smart cards, and digital media are incinerated, pulverize, or melted
- Optical disks (CDs and DVDs) are destroyed, incinerated, pulverized, crosscut shred, or melted

Change Management

Change management policies and procedures are implemented and require the documentation of approval by authorized parties and the testing of functionality prior to implementation. The party responsible for implementing the change is required to complete and submit the appropriate electronic change request to the Systems Group’s manager or the manager of the Research and Development team. Changes receive management approval by the CTO, designated officer, or

manager assigning the task. Changes are tested on a quality assurance (QA) or test network that is isolated from the production. If any discrepancies between expected and actual results that impact the network, systems, applications, business requirements, or support procedures occur, the documented back out procedures are immediately implemented. Jira tickets are used to track all changes.

Formal configuration standards are maintained for all systems in use within the environment, and systems are required to be configured appropriately prior to promotion to the production networks. All servers and network devices on PayByPhone networks are built and deployed in accordance with a system configuration policy. All production application assets are provided as Docker containers running under AWS Elastic Container Service (ECS). Select application containers are based on Alpine Linux and others are based on Microsoft Windows, and AWS resources are configured using infrastructure-as-code practices based Terraform. AWS-based components, including AWS accounts, ECS clusters, VPC networks, cloud firewalls, S3 buckets, and KMS keys are securely configured following industry best practices based on AWS and Center for Internet Security (CIS) guidance. Daily reviews are performed by the Security team to confirm that critical security configurations remain in place.

The organization maintains formally documented roles and responsibilities for personnel involved in maintaining system configuration standards. The following personnel are responsible for system configuration standards:

- The CTO or designated officer is responsible for coordinating and overseeing PayByPhone wide compliance with policies and procedures
- The Systems Group is dedicated to security planning, education, and awareness
- The Cloud Platform Infrastructure team manages PayByPhone solutions production and development environments
- The Corporate IT team is responsible for corporate user environments and services

Application Development

The organization maintains software development checklists to ensure the security during application development. The Production Readiness Checklist and the Design Review Checklist considers security, compliance, and privacy standards. Pipeline automation through GitLab CI is used to reduce the opportunities for human error in managing changes. Once approved for introduction in the various operating environments, GitLab CI performs the deployment and measures the results with pre-defined tests to ensure that common errors are caught and corrected prior to production deployments. Open Worldwide Application Security Project (OWASP) and general security best practices are always taken into account and are tracked in the Crucible code reviews. Project management methodologies like Scrum, Kanban, and Scrumban are used, and work progress is tracked in Jira.

Web application testing and sprints are used to ensure that applications are not susceptible to common vulnerabilities. Starting with writing user stories, security requirements are established by the Product Management team. As part of writing user stories, the Development team and the solutions architect are involved in shaping the security requirements. Once the stories are planned into a sprint, the Development team implements and tests the story. PayByPhone follows a test-driven development (TDD) approach, ensuring that if the security requirement can be

proven via a unit or integration test it will be, even before the implementation code change is made. If it cannot be tested with a unit or integration test, then it is tested manually, potentially with security testing tools, before it is marked as complete. Regression tests are used to identify and fix security bugs, and Dynamic analysis is performed on UI-based endpoints using the Tenable web application scanner. Jfrog scanning is built into the continuous integration and continuous delivery (CI/CD) pipeline to scan containers that are deployed in pre-production and production environments. Jfrog also runs Tenable scans on the production, development, QA, and test environments, and the scans are completed approximately every 90 days. Additionally, public-facing web applications are reviewed against, and all vulnerabilities identified are corrected; the application is to be re-evaluated after the corrections have been made.

The organization's environments for application development are logically separated. PayByPhone uses four environments as part of its software development lifecycle (SDLC): development, integration, consolidation, and production. Each environment is completely isolated and there is no connectivity between environments. Lowest level environments (development and integration) do not have outbound internet connectivity. Services in development and integration are not reachable from the internet without proper authentication. Consolidation access mimics the production environment in terms of network flow, access, IAM roles, and whitelisted AWS services.

Mechanisms and access role controls are in place to enforce the separation of duties during application development. Personnel may be granted role-based access to the pre-production environments in order for users to perform job duties; however, access to production environments is only granted on a just-in-time, time-limited basis with explicit approval using the firefighter access request process. Tasks related to coding, testing, and maintaining the production environment are separated and the company establishes a barrier between development project teams and the production environment. Developers are educated on PCI DSS, and the team stays updated on the OWASP Top 10 list and uses security testing tools when necessary. All developers are provided annual security awareness training based on OWASP content, which is provided through Inspired eLearning LMS.

Application Change Management

Code reviews are necessary to allow a change to be made in production. Code reviews are completed by an individual who did not write the code, and their review comment must indicate that they did a PCI or security assessment of the change. If an issue is found, the original coder addresses the issue and put it back through QA and completes the code review process before the code can be deployed to production. GitLab and GitHub are used to manage access to source code. Terraform code is maintained in PayByPhone's GitLab source code management repositories, and only developers have access to GitLab and GitHub. OWASP guidelines are reviewed and complied with during code reviews.

System Monitoring

Network monitoring and logging tools are installed to capture security events. AWS CloudTrail, CloudGuard, Slack, and PagerDuty are used to collect, review, analyze, and provide relevant notifications pertaining to security events within the production infrastructure. Security-related event logs are captured by the AWS, Bifrost, and Google Apigee cloud platforms. All actions

taken against AWS-based assets are captured via AWS CloudTrail, written to a dedicated S3 bucket, and reviewed by CloudGuard. Logs are retained for at least one year to support forensic reviews in the case of a security incident. Security logs are reviewed by automated log review tools to detect and notify operations personnel of potential security incidents. Check Point CloudGuard provides ongoing review and analysis of CloudTrail and other audit logs and provides notification through PagerDuty when suspicious activity is detected, and the Security team performs a daily check of CloudGuard.

Tools are installed to monitor systems to enable personnel to evaluate capacity and monitor system health. Application performance is monitored through Datadog, where numerous metrics are reviewed and analyzed. When performance is outside of expectations, Datadog generates alerts to operations through both Slack channels and PagerDuty.

Internal and external scans are conducted on a regular basis to identify potential vulnerabilities, which are prioritized and remediated based on severity. The Systems Group is responsible for conducting internal and external network vulnerability scans at least quarterly and after any significant change in the network. When internal vulnerability scans identify high-risk vulnerabilities, the issues must be remediated and rescans must be performed after remediation to verify that the high-risk vulnerabilities are resolved. External vulnerability scans must be performed by a scan vendor qualified by the payment card industry at least quarterly. When external vulnerability scans identify vulnerabilities with a CVSS score of 4.0 or higher, the issues must be remediated and rescans must be performed after remediation to verify that the vulnerabilities are resolved.

The organization conducts application and network layer penetration testing annually and following significant changes to the network. PayByPhone uses a security company that is qualified to perform internal as well as external penetration testing. The goal of penetration tests is to evaluate the security of infrastructure. Exploitable vulnerabilities are identified, remediated, and retested to verify effective remediation.

Outside sources are reviewed to identify patches and new vulnerabilities that could impact the organization's networks and systems, and patches are installed based on the criticality of the vulnerability. When security issues are identified, the Systems Group is responsible for notifying appropriate personnel, including System Administrators. The primary method for identifying new threats is through vendor and security-specific internet mailing lists. The organization subscribes to National Vulnerability Database (NVD), Microsoft, AWS, and other vendor lists applicable to PayByPhone-specific software packages and systems. New vulnerabilities are communicated through Slack, are evaluated for their impact on PayByPhone technologies, and are assigned a risk ranking. Patches for critical and high vulnerabilities must be installed within 30 days, and all other vulnerabilities are patched within three months.

Antivirus is installed on all removable media and end-user endpoints to detect and prevent the intrusion of malicious software. Microsoft Defender is configured to scan all removable media for potential malware, and it is configured to receive daily updates. Microsoft Defender antivirus is managed through Microsoft Intune, and Intune enforces the use of Defender for all Intune-managed devices, including both Windows and MacOS operating systems. As all production

application workloads are based on Docker containers, antivirus is managed by AWS on the underlying infrastructure.

Problem Management

PayByPhone maintains a formally documented Incident Response document that defines how incidents are detected and handled. The primary goal of the incident management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations. The Security Incident Response Policy outlines the initial process for reporting and responding to security events, specifically for PayByPhone information systems and operational procedures. The policy includes a comprehensive list of response team names, contacts, and responsibilities and addresses the following incident response steps:

- Identify triggering event
- Triage and start response
- Contain or isolate and mitigate
- Investigate and inform
- Remediate
- Recovery and reporting
- Lessons learned

PayByPhone has similar processes for both platform availability and for security incidents. The Sys911 Incident Response and Resolution Procedure addresses how to handle incidents that originate from the Sys911 process. Datadog is used to detect anomalies, and Sys911 is implemented in PagerDuty and Slack channels, which are monitored by on-call personnel. If the incident is a single domain (e.g., payments, vs. identity), then the incident is managed by the Service Platform team. If the incident is a multi-domain, then an incident commander is assigned. The incident commander then coordinates the incident and updates the status page. As needed to resolve the incident, the incident commander brings in additional resources and manages both internal and external communications. Once the incident is resolved, the team conducts a post-mortem exercise to identify the cause and improvements to prevent a recurrence.

Data Backup and Recovery

PayByPhone has established tools and processes to ensure backups are consistently and securely completed. The supported services for the backup solution include Amazon Aurora clusters, Amazon EBS volumes, Amazon EC2 instances, Amazon DynamoDB tables, Amazon EFS file systems, Amazon FSx file systems, and Amazon RDS databases. All backups are performed through the Amazon Web Services (AWS) RDS-provided capabilities. Backups are encrypted and stored by RDS and restore points for Oracle databases are available for one week. AWS provides capabilities to perform a point-in-time restore to any point in time within the available backups window. In the backup solution, “mps-daily-backup-plan” provides daily backups for five weeks in the managed private server (MPS) backup vault, “mps-weekly-backup-plan” offers weekly backups for three months in the MPS backup vault, and “mps-monthly-backup-plan” allows monthly backups for three months in the MPS backup vault. Backups have deletion protection and remain available even if the associated AWS resources are deleted.

The AWS Tagging Policy contains tagging policies for backups, including backup plan tag requirements. All system infrastructure is implemented through AWS-provided technologies,

and AWS CloudTrail logs are enabled and actively capturing relevant events to a dedicated AWS CloudTrail S3 bucket. The bucket is protected from accidental file deletion events and configured with a lifecycle policy to ensure retention of data.

The Disaster Recovery Plan & Business Continuity Plan is in place to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. The objective of disaster recovery process is to ensure continual operations of identified critical business systems in the event of a disaster and focuses on one-time recovery objectives in response to natural disasters, large-scale technical failures, or human threats such as attack or error. Recovery and response capabilities are built around a tiered approach (Tier 0 through Tier 4) where Tier 0 services include core AWS capabilities and application infrastructure, progressing through the other tiers based on revenue and customer impact. The overall recovery time objective (RTO) is established at 24 hours and the recovery point objective (RPO) for parking-related services is documented as 15 minutes. The Disaster Recovery Plan & Business Continuity Plan is tested and updated annually.

System Account Management

Access is provisioned to new hires based on their job role. The System Group approves access authorization based on an employee's job classification and function. A member of the Systems Group must review the Access Authorization Form to assure proper separation of duties, and contractor accounts require Systems Group approval and should automatically expire at the end of the contract. Unique user IDs are created by combining the employee's first initial with their last name.

PayByPhone has tools in place to authenticate user access to the cloud infrastructure. Azure Active Directory is used for integrated authentication to all infrastructure, including cloud-based applications and cloud service provider platforms, and to all user laptops, including both Windows and MacOS devices. Authentication is implemented for all systems and databases containing cardholder information, limiting direct SQL queries to administrators. All user identities are implemented in Azure Active Directory, and Volkswagen Financial Service (VWFS) has built and maintains Bifrost, which is an SAML-based interface for integration into all supported cloud portals used within Volkswagen. PayByPhone uses Bifrost for access to AWS Console, and all access to any in-scope system component is provided exclusively through the user's Azure Active Directory credentials.

The organization uses firefighter access, which is an example of just-in-time access management, to temporarily assign elevated access. No users have permanent, read-write administrative access to the AWS Console. When a PayByPhone employee needs elevated access to the AWS Console, they log into Bifrost and request elevated access, and the request includes a time limit. Another administrator on the approval list must approve the request, after which the requestor is granted elevated access to the AWS Console. When the time limit has expired, the requestor's access is automatically demoted to the prior access level.

Azure Active Directory is used to enforce account and password composition requirements for employees. Sessions are configured to timeout following 10 minutes of inactivity, after which

the user must re-authenticate using their password. Passwords are at least 12 characters long and must contain a combination of uppercase letters, lowercase letters, numbers, and symbols. Passwords are configured to expire and must be updated every 90 days, and the previous four passwords are remembered and cannot be re-used. Accounts are configured to lock for 30 minutes following six invalid login attempts.

The organization has tools in place to authenticate user access to the Backoffice portal. Authentication is mandated for all user IDs, system accounts, and application accounts through passwords. Clients are required to meet password composition standards when accessing the company portal, Backoffice. Standard passwords must be a minimum of 12 characters long, and System Administrator passwords must be a minimum of 16 characters long. Passwords must contain a combination of numbers, uppercase letters, and lowercase letters. Passwords are updated every 90 days, and the previous four passwords are remembered and cannot be re-used. Backoffice defines its own users and stores user credentials within the application databases using the bcrypt adaptive hashing algorithm.

PayByPhone has established a process for assigning and resetting passwords to new and existing users. The LastPass password generator is used to assign a randomly generated password to new user accounts and whenever an administrator is asked to reset a user's password. When resetting passwords, the user's identity is verified before their password is changed. System Administrators must set initial passwords that are unique and compliant with the password rules, and the password is updated by the user following the user's next login.

The organization has a process for encrypting passwords during transmission and storage. The Backoffice portal uses bcrypt for password hashing. For the cloud-based passwords, Microsoft handles the transmission of these passwords. Access is provided through Azure Active Directory-integrated single sign-on, and authentications occur using TLS-encrypted sessions under Microsoft management.

Multi-factor authentication (MFA) is used for remote access to the organization's corporate networks. The organization has implemented two distinct Azure Active Directory conditional access policies that necessitate the use of MFA during login attempts, reinforcing the authentication process with an additional layer of identity verification. The two policies enforced are the following:

- RequireMFA-MSAuth – is designed for all users across the organization; this policy necessitates the use of MFA during login attempts for access to any PayByPhone Azure Active Directory-integrated application
- One-day sign-in frequency for admins – specifically targets administrative users within the system; this policy mandates that administrators not only provide their password but also undergo MFA verification daily

PayByPhone uses Zscaler to provide remote network access to the in-scope AWS accounts and VPCs. Zscaler authentication is integrated with Azure Active Directory, which requires MFA for all authentication requests regardless of application.

Access is revoked for terminated employees, and the organization has a process for removing inactive accounts. Access is revoked immediately for terminated, transferred, or unnecessary users. Following termination, users are removed from relevant systems, including BambooHR, Azure Active Directory, and Backoffice. For inactive accounts, user IDs are disabled after 90 days of inactivity and are purged after an additional 30 days.

Risk Assessment Process

PayByPhone conducts risk assessments annually and following significant changes to the environment to identify new threats and vulnerabilities, and the NIST 800-30 methodology is followed when conducting the risk assessment. The Systems Group and the IT Operations (ITOPS) team is responsible for conducting the risk assessment, informing the company about information security issues and vulnerabilities, assigning risk ranks to the new risks and vulnerabilities, and identifying and implementing the appropriate controls to mitigate any new risks. The Jira enterprise risk management (ERM) tool is used to track both enterprise risks and IT risks, which are also captured in the risk register. Each risk is tracked separately and includes a description of the risk, risk category, likelihood, impact, risk type, and risk owner. New risks are provided to the Compliance or IT Security team through leaders of other teams. The Compliance team and IT Security team meet monthly to discuss new risks and review old ones in the Jira ERM register.

Rate limiting and geo-IP controls have been implemented through Apigee as a method to limit the risk of SMS and parking renewal bot fraud executed by external attackers against the system. Terraform and AWS Guardrails prevent misusing AWS account resources for unintended purposes, and Backoffice databases capture all events involving creating, reading, updating, and deleting application records through Backoffice, which mitigates the risk of fraud through changing the Merchant of Record information for client parking transactions.

Information and Communication Systems

The Systems Groups maintain the formally documented Information Security Policies and Procedures that define general control activities over technology. The Information Security Policies and Procedures is a single, comprehensive information security policy covering a range of topics, each in their own top-level section; the topics include the following:

- Roles and responsibilities for managing the information security program
- Change management
- Data classification and control
- Background checks
- Data retention and disposal
- Paper and electronic media
- Firewall, router, and switch security administration
- Configuration management
- Antivirus
- Backups
- Encryption of data at rest and in transit
- Software development and lifecycle management
- Incident response
- Employee identification
- Logging controls
- Service providers and third parties
- Detecting failures of critical security controls
- Internal audit of security controls
- Security awareness
- System configuration standards

The organization maintains a formally documented Security Awareness and Acceptable Use Policy that includes provisions for end-user use of PayByPhone assets. The policy defines prohibited actions pertaining to PayByPhone data and systems, and it defines critical technologies to include internet, intranet, and extranet-related systems, including computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and File Transfer Protocol (FTP).

The policies and procedures define the information security responsibilities for personnel. The Systems Groups, including Cloud Platforms and Corporate IT, are responsible for detailed policies and procedures as well as implementation of controls on PayByPhone's information systems, reviewing relevant information security logs, and administering user accounts, among other responsibilities. Users are responsible for understanding the consequences of their actions, maintaining awareness of policies, attending security awareness training, and remaining knowledgeable of data classification and handling requirements.

Vendor Management

PayByPhone has a process in place for establishing and maintaining a relationship with vendors and services. Due diligence is performed prior to the selection of new vendors or service providers. PayByPhone engages with a vendor for proof of concept (POC) early in the process, and during this process PayByPhone acquires the vendor's compliance documentation, such as ISO 27000, SOC 2, and PCI AOC. If the vendor cannot provide appropriate audit reports, PayByPhone engages in a vendor risk assessment; the process is ad-hoc and tailored to the individual vendor. A mutual non-disclosure agreement (NDA) is established that binds PayByPhone and the vendor to maintain confidentiality, and the agreement requires that the receiving party protects the information with reasonable care and consistent with the measures it would take to protect its own confidential information. PayByPhone annually reviews all critical vendors and gathers the most recent audit reports, such as ISO 27000, SOC 2, and PCI DSS; when reviewing the SOC 2 exceptions, reasonable controls, and the opinion are reviewed.

Monitoring Controls

PayByPhone has monitoring activities in place to ensure operational quality and control. Operational quality and control are managed through site reliability management (SRM) principles, which create a framework for the observability of IT systems and the related incident or service management processes and metrics to monitor the service. The SRM is responsible for establishing reliability expectations for all other engineering teams to follow, including internal service-level agreements (SLAs) (99.9%). In some cases, SLAs can also be committed to external customers. Jira tickets are used to track operational errors experienced in the production environment, and Datadog is used to monitor various services within the production application and to notify operations staff via PagerDuty. Datadog provides metrics and dashboards accessible to both business and technical staff. The metrics monitored include transaction and order processing metrics with a focus on credit card processing metrics tracking the number of transactions, including both successful and unsuccessful, and platform reliability (site reliability) metrics that track platform availability across the PayByPhone technology components.

Real-time monitoring of payment transactions is in place, with alerts triggered for a specified number of failures or declines over a specific timeframe. Alerts are sent via PagerDuty to the on-

call PayByPhone support personnel, who assess and address the issue, often by disabling suspicious motorist accounts. Project monitoring is facilitated through Confluence, and regular project updates are provided to the Executive team. PayByPhone uses the Payment Processor Runbook to diagnose and remediate various processing errors that can occur on the platform.

Changes to the System During the Period

The following changes, which are likely to affect report users’ understanding of the payment processing services system, occurred during the period from November 1, 2022, through October 31, 2023.

Description of Change	Effect of the Change on the System	Date of Change
PayByPhone migrated data center-applications and infrastructure to AWS.	<p>Auditor learned through interviews that PayByPhone recently transitioned all applications out of a contracted colocation facility and into AWS. This transitioned resulted in numerous operational changes as PayByPhone transitioned from the legacy, virtual machine-based delivery model to one that is based almost entirely on modern DevOps principles using cloud-provided infrastructure.</p> <p>During the decommissioning process, PayByPhone commissioned Dataknox.io to destroy all media from data center-located systems.</p>	Ongoing throughout the audit period, with final completion May 2023
PayByPhone was sold Volkswagen Financial Services (VWFS) to FLEETCOR	There were no meaningful changes within this audit period as a direct result of the sale; however, future changes could be expected in the implementation of controls currently performed by VMFS.	September 2023

COMPLEMENTARY USER-ENTITY CONTROLS

PayByPhone's services are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. PayByPhone's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. PayByPhone also provides best practice guidance to clients regarding control element outside the sphere of PayByPhone responsibility.

This section describes additional controls that should be in operation at user organizations to complement the PayByPhone controls. Client Consideration recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with PayByPhone.
- User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with PayByPhone's services.
- Transactions for user organizations relating to PayByPhone's services should be appropriately authorized, and transactions should be secure, timely, and complete.
- For user organizations sending data to PayByPhone, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
- User organizations should implement controls requiring additional approval procedures for critical transactions relating to PayByPhone's services.
- User organizations should report to PayByPhone in a timely manner any material changes to their overall control environment that may adversely affect services being performed by PayByPhone.
- User organizations are responsible for notifying PayByPhone in a timely manner of any changes to personnel directly involved with services performed by PayByPhone. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by PayByPhone.
- User organizations are responsible for adhering to the terms and conditions stated within their contracts with PayByPhone.
- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by PayByPhone.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION IV: TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

APPLICABLE TRUST SERVICES CRITERIA RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY, AND PROCESSING INTEGRITY

Although the applicable trust services criteria and related controls are presented in section IV, “Trust Services Categories, Criteria, Related Controls, and Tests of Controls,” they are an integral part of PayByPhone’s system description throughout the period November 1, 2022, to October 31, 2023.

Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization’s ability to achieve its service commitments and system requirements.

Security refers to the protection of

- i. information during its collection or creation, use processing, transmission, and storage and
- ii. systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of PayByPhone’s service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

The trust services criteria relevant to availability address the need for information and systems to be available for operation and use to achieve the service organization’s service commitments and system requirements.

Availability refers to the accessibility of information used by PayByPhone’s systems, as well as the products or services provided to its customers. While the availability objective does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems), it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Processing Integrity

The trust services criteria relevant to processing integrity address the need for system processing to be complete, valid, accurate, timely, and authorized to achieve the service organization’s service commitments and system requirements.

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for

which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.

Confidentiality

The trust services criteria relevant to confidentiality address the need for information designated as confidential to be protected to achieve the service organization's service commitments and system requirements.

Confidentiality addresses PayByPhone's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from PayByPhone's control in accordance with management's objectives. Information is confidential if the custodian of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties. Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories

Control Environment

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	The organization relies on leadership and conducts training to ensure that security and compliance are prioritized.	<p>Interviewed the Manager of Security and IT Compliance and determined that the primary directive from management is to ensure compliance; the primary method to achieve this is through education; the compliance program is enforced through a quarterly presentation between the Compliance team and leadership to cover the top five initiatives; and the organization communicates every compliance effort to the PayByPhone Product Steering Board (PSB) to ensure that the compliance program contributes to corporate value</p> <p>Observed Weekly Cyber Posts, townhall meetings notes, and IT security blogs and verified that continuous training is provided to develop a security and compliance-conscious culture</p>	No Relevant Exceptions Noted
CC1.1.2	Corporate policies and company handbooks are used to communicate guidelines and company expectations.	<p>Reviewed the Global Guidelines document and verified that it addresses the following policies:</p> <ul style="list-style-type: none"> • Crisis Communication Guidelines • Guideline for analyzing and reporting a data breach to the authorities and data subjects • Data Subject Request Guideline • PayByPhone Compliance Requirements Overview <p>Reviewed the Global Policies document and verified that it shows top-level principles on specific subject matters, and the following policies are addressed:</p> <ul style="list-style-type: none"> • Data Protection Policy • Data Retention Policy • Global Information Security Policies 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Security Incident Response Policy • Background Check Policy <p>Reviewed the North American Organizational Handbook and verified that it addresses the following North American policies and guidelines:</p> <ul style="list-style-type: none"> • Remote Work Health & Safety Policy • Sick & Personal Time Off Policy • Time Off Vacation Policy • Equal Employment Opportunity Policy <p>Interviewed the People Business & Operations Partner and determined that the Employee Handbook is maintained in Confluence</p> <p>Observed records for a sample of new hires (4 of 44) and verified that handbooks are acknowledged by new employees</p>	
CC1.1.3	<p>A Code of Conduct is maintained that communicates company values as well as ethical and behavioral expectations to employees.</p>	<p>Reviewed the VWFS Code of Conduct and verified that it includes:</p> <ul style="list-style-type: none"> • Messages regarding integrity and compliance • Social responsibility • Responsibilities to business partners • Commitments to other teammates • Occupational safety and healthcare • Data protection • Security and protection of information • Know-how and intellectual property • IT security • Handling company assets <p>Interviewed the Manager of Security and IT Compliance and determined that the core values of the company are:</p> <ul style="list-style-type: none"> • See through customers' eyes • Work together • Stay curious 	<p>No Relevant Exceptions Noted</p>

		<ul style="list-style-type: none"> • Have fun • Make things happen <p>Observed records for a sample of new hires (4 of 44) and verified that the onboarding checklist items, including acknowledgement of all company policies and Code of Conduct</p>	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	A management board (M-Board) is established to provide oversight and direction to the organization.	<p>Interviewed the Manager of Security and IT Compliance and determined that the management consists of the Chief Executive Officer (CEO), Chief Financial Officer (CFO), and Chief Technology Officer (CTO)</p> <p>Interviewed the Chief information Security Officer (CISO) & Senior Director of Reliability and determined that the PayByPhone management board (M-Board) consists of the PayByPhone CEO, CTO, and CFO</p> <p>Observed three monthly M-Board agendas and verified that compliance and information security topics are covered, and that the M-Board monthly meeting is established on a regular cadence</p>	No Relevant Exceptions Noted
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	Organization charts are maintained that illustrate the separation of duties, company structure, and reporting lines.	Interviewed the Manager of Security and IT Compliance and determined that Security and IT Compliance reports through the CTO organization as one of three permanent PayByPhone board members (CEO, CTO, and CFO); a process is in place to ensure that certain activities, such as decisions and transaction choices, must be approved by at least two people, and this controlling mechanism is used to facilitate delegation of authority and increase transparency	No Relevant Exceptions Noted

		<p>Observed the organization chart and verified that it illustrates the reporting lines, company structure, and separation of duties, and that the company senior leadership consists of the CEO, CFO and CTO, who are responsible for all day-to-day operations of the company</p> <p>Observed the company’s organization charts in BambooHR and verified that the senior leadership consists of the CEO, CTO, and CFO</p>	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	The organization maintains formally documented job descriptions for personnel.	Observed numerous job descriptions for information security personnel, including CISO & Manager of Compliance and IT Security, Software Engineers, and Security Analysts, and verified that information security concerns were appropriate to each role	No Relevant Exceptions Noted
CC1.4.2	Onboarding activities are outlined in the Employee Onboarding Checklist and are managed in BambooHR to ensure all employees are consistently onboarded.	<p>Interviewed the People Business & Operations Partner and determined that onboarding is managed on the Employee Onboarding Checklist on BambooHR and includes tax forms, eligibility forms, payroll forms, bank deposits, protection of corporate interests agreement, and technology onboarding; all employees sign a confidentiality agreement as part of their employment agreement</p> <p>Observed the onboarding task list and verified that the manager’s role in the onboarding process includes preparing an onboarding plan, forwarding recurring calendar invites and inviting the new team member to appropriate Slack channels, and communicating the laptop requirements to the talent acquisition partner; the employee’s tasks in the onboarding process involve reviewing the health and safety information, reviewing the organizational handbook and code of conduct, reviewing the day one orientation files and bookmarking</p>	No Relevant Exceptions Noted

		<p>links, and reviewing and signing the company policies</p> <p>Observed records for a sample of new hires (4 of 44) and verified that the following items are completed:</p> <ul style="list-style-type: none"> • BambooHR Onboarding Checklist • Access request tickets in Jira • Background checks results • Completion of security awareness training • Information security policy acknowledgements <p>Observed the Confidentiality Agreement and verified that they address the terms and conditions of employment with PayByPhone; the agreement mentions issues related to confidentiality, non-competition, non-solicitation, and ownership of work product</p>	
CC1.4.3	All potential employees undergo a background check before being hired.	<p>Reviewed the Information Security Policies and Procedures (dated September 4, 2023) and verified the following:</p> <ul style="list-style-type: none"> • The background check policy applies to all employees and contractors with access to cardholder data • PayByPhone aims to perform background checks for all employees, but there may be exceptions for new residents • Checks should include verification of name, address, and date of birth • Official identification and Social Security number verification is required • Employment and educational verification should be conducted • Credit checks, federal or state criminal record checks, and reference checks are necessary • Drug screenings may be applicable and allowed by law 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Protections for PII and background check results are in place <p>Interviewed the People Business & Operations Partner and determined that background checks are performed by Sterling in accordance with all local laws and regulations</p> <p>Observed new hire records for a sample of new employees (4 of 44) and verified that the background checks were completed by Sterling</p>	
CC1.4.4	<p>Training and continuous education opportunities are provided to employees via the Inspired eLearning learning management system (LMS).</p>	<p>Reviewed the Security & IT Compliance Onboarding document and verified all new employees must attend and acknowledge completion of the organization’s Security Program, which addresses the following:</p> <ul style="list-style-type: none"> • Awareness training • Risk assessment • Policies and procedures • Business case studies • What is a Security Incident? • Examples of non-public private information (NPPI) • Indications of an attack (security event) • Examples of confidentiality, integrity, and availability incidents • How to respond to when a security incident is detected <p>Interviewed the Manager of Security and IT Compliance and determined that general security awareness training is provided through the Inspired eLearning LMS, and new campaigns are run quarterly to keep training fresh and short for all users; all new hires are provided security awareness training on a bi-monthly schedule where the session is conducted as a live-session (in-person or through web conference, as appropriate)</p>	<p>No Relevant Exceptions Noted</p>

		<p>Observed that Security and Compliance team members hold various certifications and verified that some of the certifications include the following:</p> <ul style="list-style-type: none"> • GIAC Security Essentials (SANS Technology Institute) • GIAC Certified Incident Handler (SANS Technology Institute) • GIAC Public Cloud Security (SANS Technology Institute) • EXIN Information Security ISO 27001 Certificate • CompTIA Cloud Essentials+ certificate • ITIL & RSA Incident Handling <p>Observed the use of Inspired eLearning and verified that it is used to provide security awareness content to all employees, and that the LMS also captures each user’s acknowledgement of their receipt and understanding of the information security policy</p>	
CC1.4.5	<p>The organization has a process in place that outlines how to complete voluntary and involuntary terminations.</p>	<p>Interviewed the People Business & Operations Partner and determined the following:</p> <ul style="list-style-type: none"> • In the event of voluntary termination, the employees must provide a 30-day notice, as stipulated in the Employment Agreement, but the organization attempts to accommodate shorter if needed • The termination process begins in BambooHR and requires submitting a “Joiners and Leavers” ticket in Jira to manage the process with all parties • In the event of involuntary termination, a similar process is followed, but with greater urgency in coordination between all the parties • In both cases, equipment is returned through a courier service and compared against IT asset inventory 	<p>No Relevant Exceptions Noted</p>

		<ul style="list-style-type: none"> The termination process is managed in BambooHR and Jira tickets <p>Observed offboarding records for a sample of terminated employees (9 of 93) and verified that the employees were removed from all relevant systems, including BambooHR, Azure Active Directory, and Backoffice</p>	
CC1.4.6	Personnel with application development responsibilities participate in industry-specific training.	<p>Interviewed the Manager of Security and IT Compliance and determined that developers are educated on Payment Card Industry Digital Security Standards (PCI DSS); the team stays updated on the Open Worldwide Application Security Project (OWASP) Top 10 list and uses security testing tools when necessary; and all developers are provided annual security awareness training based on OWASP content, which is provided through InspiredLearning LMS</p> <p>Observed completion roster for InspireLearning and verified that developers completed the relevant training</p>	No Relevant Exceptions Noted
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	Performance evaluations and reviews are completed on a regular basis to ensure expectations are being met.	<p>Interviewed the People Business & Operations Partner and determined that ongoing one-on-ones with managers on a frequency established by the employee and manager; coaching between employees and leadership when performance expectations are not being met (January and July); and salary reviews are performed annually (February for North America and March for Europe)</p> <p>Observed the use of BambooHR to manage employees and verified that BambooHR captures the performance evaluation process</p>	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Communication and Information			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	The organization has monitoring activities in place to ensure operational quality and control.	<p>Interviewed the Manager of Security and IT Compliance and determined that operational quality and control is managed through site reliability management (SRM) principles, which create a framework for the observability of IT systems and the related incident or service management processes and metrics to monitor the service; the SRM is responsible for establishing reliability expectations for all other engineering teams to follow, including internal service-level agreements (SLAs) (99.9%); in some cases, SLAs can also be committed to external customers, but this is not the default</p> <p>Observed Jira tickets from operational errors experienced in the production environment and verified tickets are used in response to application failures, which led to diminished performance, including failed payment processing functions</p> <p>Observed the use of Datadog and verified that it is used to monitor various services within the production application and to notify operations staff via PagerDuty</p> <p>Observed use of the SRM dashboards through Datadog to monitor site performance and verified that the following metrics are monitored:</p> <ul style="list-style-type: none"> Transaction and order processing metrics with a focus on credit card processing metrics tracking the number of transactions, 	No Relevant Exceptions Noted

		<p>including both successful and unsuccessful</p> <ul style="list-style-type: none"> Platform reliability (site reliability) metrics, which track platform availability across the PayByPhone technology components 	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	<p>Leadership maintains continuous communication with employees, including meetings and emails, to ensure employees are aware of the tone and direction of the company.</p>	<p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> The organization conducts monthly business update meetings, conducts weekly all-hands meeting, distributes weekly development and product news emails, and holds development and product quarterly townhall meetings The organization conducts quarterly leadership reviews with the management board (CEO, CTO, and CFO), conducts quarterly development townhall meetings, completes monthly business update reports, and conducts weekly one-on-one meetings between Compliance and the CISO & Senior Director of Reliability <p>Observed Teams invites for Friday meetings and verified that development and production leader meetings occur weekly</p> <p>Observed an email that was distributed to all staff (dated December 2022) and verified that all-hands meetings are conducted quarterly</p> <p>Observed a Teams invite for the monthly Global Leadership Forum (dated April 3, 2023) and verified that the organization conducts monthly leadership meetings</p>	<p>No Relevant Exceptions Noted</p>

		<p>Observed all-hands meeting materials and verified that key messages are delivered from the leadership to all employees</p> <p>Observed all-hands meeting materials for developers and production personnel and verified that platform engineering and operations personnel are informed of key messages as they relate to the specific duties</p> <p>Observed an email that addressed management team updates (dated January 19, 2023) and verified that it communicated personnel changes to the company</p>	
CC2.2.2	The organization maintains formally documented incident response procedures that define the roles and responsible for personnel when handling incidents.	<p>Reviewed the Incident Response document and verified that the primary goal of the incident management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations; the plan addresses the roles and responsibilities of the business user, the on-call engineer, SRM, and InfoSec (SecOps)</p> <p>Reviewed the Security Incident Response Policy and verified that it outlines requirements, policy statements, and initial process for reporting and responding to security events, specifically for PayByPhone information systems and operational procedures; the policy includes a comprehensive list of response team name, contacts, and responsibilities:</p> <ul style="list-style-type: none"> • Security Incident Response • Architecture Delegate • Platform Infrastructure Delegate • IT Compliance Manager • Legal Counsel, Compliance • Data Protection <p>Interviewed the Manager of Security and IT Compliance and determined that the core incident response team consists of Security and Compliance</p>	No Relevant Exceptions Noted

		<p>Team members and senior technical leadership; the team is responsible for both security as well as platform availability incidents</p> <p>Observed that the incident response commanders are also part of the SYS911 platform response team and verified that the Security team provides security incident response support as needed based on the type of incident, and the incident response teams also consist of other technical expertise as needed based on the type of the incident</p> <p>Observed that security incident response training is provided for the Security and Compliance team members and verified Udemmy course completion certificates for the following:</p> <ul style="list-style-type: none"> • Manager of Security and IT Compliance • Information Security Analyst • Information Security Lead 	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	The organization has a process for communicating incidents to impacted personnel and clients.	<p>Reviewed the Ongoing Outage Response Guide and verified that it addresses the following steps for reporting incidents:</p> <ul style="list-style-type: none"> • Step 1: Impact Analysis • Step 2: Escalation • Step 3: Root Cause Analysis • Step 4: Communication • Step 5: Remediation • Step 6: “All Clear” Communication • Step 7: Next Steps <p>Reviewed the Ongoing Outage Response Guide and verified that it outlines the steps for reporting incident steps and communicating the impact of the incident with relevant people</p>	No Relevant Exceptions Noted

		Observed the PayByPhone status page and verified that it includes a live status update for PayByPhone systems	
CC2.3.2	Contractual materials are used to communicate descriptions of services to the organization's clients.	<p>Observed three contracts and verified that the contracts include the following:</p> <ul style="list-style-type: none"> • Intellectual property rights • Definition and responsibilities pertaining to client data • Definition and responsibilities pertaining to customer (parker) data • Mutual indemnification • Mutual confidentiality and non-disclosure • Survival of specific clauses in the event of contract termination (specifically, confidentiality, intellectual property and indemnification clauses) • PayByPhone responsibility to maintain PCI DSS compliance 	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories

Risk Assessment

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	The organization adheres to regulatory measures that impact its operations.	<p>Reviewed the Data Protection Policy and verified that it establishes the organization's process of managing the availability, usability, integrity, and security of the data in enterprise systems in accordance with all legal, regulatory, compliance, and business requirements</p> <p>Interviewed the Manager of Security and Compliance and determined that PayByPhone adheres to the following business and regulatory compliance requirements:</p> <ul style="list-style-type: none"> • Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) • Canadian Consumer Privacy Protection Act (CPPA) • European Union General Data Protection Regulation (GDPR) • PCI DSS • California Consumer Privacy Act (CCPA) 	No Relevant Exceptions Noted
CC3.1.2	The organization maintains policies and procedures for addressing a customer's privacy rights.	<p>Reviewed the Guideline for Analyzing and Reporting a Data Breach to the Authorities and Data Subjects document and verified that it outlines the handling or notification of appropriate stakeholders in the event of a data breach necessary to comply with the GDPR requirements</p> <p>Reviewed the Data Protection Impact Assessment (DPIA) Process (dated May 2021) and verified that the DPIA is an important component of the risk-oriented approach in data protection; a DPIA is conducted to ensure that targeted measures can be found to contain risk</p>	No Relevant Exceptions Noted

		Observed the organization’s online Privacy Policy located on the company website and verified that it addresses data subjects rights under the GDPR and CCPA	
CC3.1.3	The organization conducts an annual risk assessment based on specified company objectives.	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that the Systems Group and the IT Operations (ITOPS) team does the following:</p> <ul style="list-style-type: none"> • Conducts an annual formal risk assessments to identify new threats and vulnerabilities • Informs the company about information security issues and vulnerabilities • Monitor and identifies new security vulnerabilities and assigns risk ranks to them <p>Interviewed the Manager of Security and IT Compliance and determined that the Compliance team reviews all risks monthly</p> <p>Interviewed the Manager of Security and Compliance and determined the following:</p> <ul style="list-style-type: none"> • At least annually, the organization coordinates a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks • Security risk assessments are reported and are shared with the Board on a quarterly basis • Vulnerabilities are assigned a risk ranking, and the risks levels include “high risk” and “critical” • The organization uses the Jira enterprise risk management (ERM) tool to track all risks in the risk register • Both enterprise risks and IT risks are tracked • Each risk is tracked separately and includes a description of the 	No Relevant Exceptions Noted

		<p>risk, risk category, likelihood, impact, risk type, and risk owner</p> <ul style="list-style-type: none"> • New risks are provided to the Compliance team or IT Security team through leaders of other teams • The Compliance team and the IT Security team meet monthly to discuss new risks and review old ones in the Jira ERM register • National Institute of Standards and Technology (NIST) 800-30 methodology is followed <p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p> <p>Observed the use of Jira IT assets and verified that it is used to track all assets such as Amazon Web Services (AWS) accounts, ECS clusters, and databases used within the system</p> <p>Observed the Jira ERM risk tickets and verified that legal, compliance, and IT risks are followed</p> <p>Observed the Q2 2023 risk register results and verified that the risk register is maintained and includes updates for resolved risks, newly identified risks, and current risks</p>	
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
CC3.2.1	The organization tracks and ranks enterprise and IT risks based on likelihood and impact.	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that the Systems Group and ITOPS team conducts an annual formal risk assessments to identify new threats and vulnerabilities</p> <p>Interviewed the Manager of Security and IT Compliance and determined that the Compliance team reviews all risks monthly</p>	No Relevant Exceptions Noted

		<p>Interviewed the Manager of Security and Compliance and determined the following:</p> <ul style="list-style-type: none"> • Both enterprise risks and IT risks are tracked • Vulnerabilities are assigned a risk ranking, and the risks levels include “high risk” and “critical” • Each risk is tracked separately and includes a description of the risk, risk category, likelihood, impact, risk type, and risk owner <p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p>	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	<p>Risks relating to fraud are assessed as part of the annual risk assessment.</p>	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that a risk assessment is required to be performed at least annually</p> <p>Interviewed the Manager of Security and IT Compliance and determined that the Compliance team reviews all risks monthly</p> <p>Observed that rate limiting and geo-IP controls have been implemented through Apigee as a method to limit the risk of SMS and parking renewal bot fraud executed by external attackers against the system</p> <p>Observed the use of Terraform and AWS Guardrails and verified that they prevent misusing AWS account resources for unintended purposes</p> <p>Observed Backoffice databases capture all events involving creating, reading, updating, and deleting application records through Backoffice, which mitigates the risk of fraud through changing the Merchant of Record information for client parking transactions</p>	<p>No Relevant Exceptions Noted</p>

		<p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p> <p>Observed the risk register from Q2-2023 and verified that examples of risks pertaining to fraud were captured in the register</p>	
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	The organization performs a risk assessment following any significant changes to the environment.	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that the Systems Group and ITOPS team performs risk assessments when significant changes occur in the environment</p> <p>Interviewed the Manager of Security and IT Compliance and determined that the Compliance team reviews all risks monthly</p> <p>Interviewed the Manager of Security and Compliance and determined that risk assessments are performed upon significant changes to the environment</p> <p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p>	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Monitoring Activities			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC4.1.1	The organization undergoes regulatory audits annually.	<p>Interviewed the Manager of Security and IT Compliance and determined that SOC 2 and PCI audits are performed by KirkpatrickPrice</p> <p>Observed completed SOC 2 and PCI reports and verified that the organization undergoes annual audits</p>	No Relevant Exceptions Noted
CC4.1.2	Risks are evaluated to determine the effectiveness of selected internal controls.	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that the Systems Group and ITOPS team does the following:</p> <ul style="list-style-type: none"> • Conducts an annual formal risk assessments to identify new threats and vulnerabilities • Informs the company about information security issues and vulnerabilities • Monitors and identifies new security vulnerabilities and assigns risk ranking to them • Uses reputable outside sources for vulnerability information • Subscribes to vendor and security-specific internet mailing lists for threat identification • Maintains updates and patches for operating systems and applications <p>Interviewed the Manager of Security and Compliance and determined the following:</p> <ul style="list-style-type: none"> • At least annually, the organization coordinates a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Security risk assessments are reported and are shared with the Board on a quarterly basis • Vulnerabilities are assigned a risk ranking, and the risks levels include “high risk” and “critical” • The Compliance team reviews all risks monthly <p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p>	
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
CC4.2.1	Monitoring and alerting tools are installed to detect and notify staff of internal deficiencies.	<p>Observed Jira tickets from operational errors experienced in the production environment and verified that the tickets were filed in response to application failures which led to diminished performance, including failed payment processing functions</p> <p>Observed the use of Datadog and verified it is used to monitor various services within the production application and to notify operations staff via PagerDuty</p>	No Relevant Exceptions Noted
CC4.2.2	The relevant teams conduct regular meetings to discuss risk rankings and mitigation strategies.	<p>Interviewed the Manager of Security and Compliance and determined the following:</p> <ul style="list-style-type: none"> • Security risk assessments are reported and are shared with the Board on a quarterly basis • The Compliance team and IT Security team meet monthly to discuss new risks and review old ones in the Jira ERM register • The Compliance team reviews all risks monthly <p>Observed risk meeting minutes and verified that semi-monthly updates have occurred since December 2022 and most recent September 7, 2023; the meeting discussion topics include a review of new risks, a review of top risks, and a review of quarter security report</p>	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Control Activities			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	The organization maintains a formally documented Security Awareness and Acceptable Use Policy that outlines the guidelines for users who use company assets.	<p>Reviewed the Security Awareness and Acceptable Use Policy and verified that it includes provisions for end-user use of PayByPhone assets; it defines prohibited actions pertaining to PayByPhone data and systems; it defines critical technologies to include internet, intranet, and extranet-related systems, including computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and File Transfer Protocol (FTP)</p> <p>Interviewed the Manager of Security and IT Compliance and the People Business & Operations Partner and determined that all personnel must acknowledge the policy as part of the overall PayByPhone policy set upon new hire</p> <p>Observed onboarding records for a sample of new hires (4 of 44) and verified that new hires review and acknowledge policies</p>	No Relevant Exceptions Noted
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	The Systems Groups maintain the formally documented Information Security Policies and Procedures that define general control activities over technology.	<p>Reviewed the Information Security Policies and Procedures is a single, comprehensive information security policy covering a range of topics, each in their own top-level section; topics include:</p> <ul style="list-style-type: none"> • Roles and responsibilities for managing the information security program • Change management • Data classification and control 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Background checks • Data retention and disposal • Paper and electronic media • Firewall, router, and switch security administration • Configuration management • Antivirus • Backups • Encryption of data at rest and in transit • Software development and lifecycle management • Incident response • Employee identification • Logging controls • Service providers and third parties • Detecting failures of critical security controls • Internal audit of security controls • Security awareness • System configuration standards <p>Interviewed the Manager of Security and IT Compliance, the Information Security Lead, the CISO & Senior Director of Reliability, and the Information Security Analyst and determined the following:</p> <ul style="list-style-type: none"> • The Systems Groups, including Cloud Platforms and Corporate IT, are responsible for detailed policies and procedures as well as implementation of controls on PayByPhone’s information systems, reviewing relevant information security logs, and administering user accounts, among other responsibilities • Users are responsible for understanding the consequences of their actions, maintaining awareness of policies, attending security awareness training, and remaining knowledgeable of data classification and handling requirements 	
--	--	--	--

		<p>Observed the use of Confluence and verified that it is used distribute information security policies to all parties</p> <p>Observed onboarding records for a sample of new hires (4 of 44) and verified that new hires review and acknowledge policies</p>	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	<p>The organization has a process for continuously reviewing and updating the Information Security Policies and Procedures.</p>	<p>Interviewed the Manager of Security and IT Compliance and determined that the Security team is responsible for creating and updating policies, and management is responsible for policy approval</p> <p>Interviewed the Manager of Security and IT Compliance, the Information Security Lead, the CISO & Senior Director of Reliability, and the Information Security Analyst and determined the following:</p> <ul style="list-style-type: none"> • The organization has a monolithic information security policy that includes an internal review and approval • PayByPhone maintains an information security policy in Jira as Information Security Policies and Procedures • As a Jira-based document, it is continuously updated as needed; the CTO, or their designee, is responsible for managing the information security policy; and in practice, this responsibility is assigned to the CISO and primarily executed by the Manager, Security, and IT Compliance • The policy is reviewed annually by the M-Board before incorporating into the Global Organization Handbook <p>Observed at least eight minor policies updates that were made within the</p>	<p>No Relevant Exceptions Noted</p>

		<p>audit period and verified that the policies and procedures are continuously updated</p> <p>Observed the use of Confluence and verified that it is used distribute information security policies to all parties</p>	
--	--	---	--

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories

Logical and Physical Access Controls

Ctrl #	Description of Controls	Service Auditor’s Tests of Controls	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives.		
CC6.1.1	The organization has tools in place to authenticate user access to the cloud infrastructure.	<p>Reviewed the Information Security Policies and Procedures and verified that authentication is implemented for all systems and databases containing cardholder information, limiting direct SQL queries to administrators</p> <p>Observed all user identities are implemented in Azure Active Directory and that Volkswagen Financial Service (VWFS) has built and maintains Bifrost, which is a SAML-based interface for integration into all supported cloud portals used within Volkswagen, and verified that PayByPhone currently uses Bifrost for access to AWS Console; therefore, the authentication hierarchy when an administrator needs to access the AWS Console is as follows: AWS Console – > Bifrost –> Azure Active Directory where all identities are derived from Azure Active Directory</p> <p>Observed SAML integration configurations for Bifrost, Azure Active Directory, AWS Console, and Google Cloud and verified that all access to any in-scope system component is provided exclusively through the user’s Azure Active Directory credentials</p> <p>Observed that elevated access is managed through a just-in-time provisioning system in Bifrost; an engineer with the ability to request elevated access must submit firefighter request, which is approved by another person on the authorized approvers</p>	No Relevant Exceptions Noted

		<p>list, after which the access is granted on a temporary, time-bound basis</p> <p>Observed the firefighter log and verified that all firefighter access requests are logged</p> <p>Observed the use of the firefighter access feature in Bifrost to grant just-in-time access to cloud system administrator</p>	
CC6.1.2	<p>The organization has tools in place to authenticate user access to the Backoffice portal.</p>	<p>Interviewed the Manager of Security and IT Compliance and determined that authentication is mandated for all user IDs, system accounts, and application accounts through passwords</p> <p>Observed the Backoffice application and verified that it defines its own users and stores user credentials within the application databases using the bcrypt adaptive hashing algorithm</p> <p>Observed user accounts for the Backoffice application and verified that accounts are hashed using bcrypt prior to storage in the application database</p> <p>Observed application configuration settings and verified that bcrypt is used with a cost factor of 12, a system-specific pepper and salt length of 16 bytes</p>	<p>No Relevant Exceptions Noted</p>
CC6.1.3	<p>All users are assigned a unique user ID prior to accessing system components.</p>	<p>Interviewed the Manager of Security and IT Compliance and determined that unique user IDs are formed by combining the employee's first initial with their last name</p> <p>Observed that Azure Active Directory is used for integrated authentication to all infrastructure, including cloud-based applications and cloud service provider platforms, and to all user laptops including both Windows and MacOS devices</p>	<p>No Relevant Exceptions Noted</p>

CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
CC6.2.1	Access rights and privileges are provisioned to new hires and contractors based on their job role.	<p>Reviewed the Information Security Policies and Procedures and verified that access to data is assigned based on least privilege; System Group approves access authorization based on an employee’s job classification and function; a member of the Systems Group must review the Access Authorization Form to assure proper separation of duties; and contractor accounts require Systems Group approval and should automatically expire at the end of the contract</p> <p>Observed a demonstration of Azure Active Directory role assignments for user accounts and verified that those ending in “-SA” are exclusively assigned to Azure Active Directory roles</p> <p>Observed Jira tickets for a sample of new hires (4 of 44) and verified that Jira tickets include approval prior to implementation</p> <p>Observed access requests to Azure Active Directory group permissions and verified that provisioned access is consistent with documented approvals</p> <p>Observed roles for general users, system administration, and other purposes are defined in the Access Control Matrix in the Information Security Policies and Procedures Jira page and verified that the Access Control Matrix includes the following defined roles:</p> <ul style="list-style-type: none"> • Basic User • Support • Manager • Developer • System Administrator • Security Administrator 	No Relevant Exceptions Noted

<p>CC6.2.2</p>	<p>The organization has a process for managing passwords, including resetting passwords and assigning first-time passwords.</p>	<p>Reviewed the Demonstrate Password Reset Procedures document and verified that the reset password process is completed in Microsoft Azure</p> <p>Interviewed the Manager of Security and IT Compliance and determined the following regarding password resets:</p> <ul style="list-style-type: none"> • System Administrators must validate the identity of users before performing a password reset • Passwords are set by System Administrators and must be changed by the user immediately upon the user's next login • System Administrators must set initial passwords that are unique and compliant with the password rules <p>Observed the use of the LastPass password generator to assign a randomly generated password to new user accounts and when an administrator is asked to reset a user's password</p> <p>Observed new user account passwords and verified that password reset requests use a randomly generated password</p> <p>Observed the use of first-time passwords and password reset requests and verified that both use randomly assigned passwords</p> <p>Observed system administrators through the first-time password and password reset processes and verified that random passwords are created using LastPass' password generator feature</p>	<p>No Relevant Exceptions Noted</p>
<p>CC6.2.3</p>	<p>The organization uses Azure Active Directory to enforce password composition requirements for employees.</p>	<p>Reviewed Information Security Policies and Procedures (dated July 11, 2023) and verified that user authentication procedures require unique user accounts, passwords or</p>	<p>No Relevant Exceptions Noted</p>

		<p>token entry, and acknowledgement of security policies, and passwords are at least 12 characters long, complex, and changed every 90 days</p> <p>Observed that all password policies are enforced in Azure Active Directory and include minimum password length, expiry, complexity, and reuse provisions:</p> <ul style="list-style-type: none"> • Minimum password length is eight-character passwords (PayByPhone policy requires 12 characters, but Azure Active Directory is limited to eight) • Passwords consist of a combination of uppercase and lowercase characters • Passwords cannot include family names, phone numbers, car registration numbers, company name, usernames, or birthdays • The previous four passwords are remembered and cannot be re-used • Passwords are changed every 90 days 	
CC6.2.4	<p>Clients are required to meet password composition standards when accessing Backoffice.</p>	<p>Reviewed the Information Security Policies and Procedures and verified that System Administrators set initial passwords that comply with password rules, and users must change them upon login; identity verification is required for password resets, using approved methods such as face-to-face or remote procedures</p> <p>Interviewed the Manager of Security and IT Compliance and determined that passwords adhere to the following standards:</p> <ul style="list-style-type: none"> • Standard passwords are minimum of 12 characters long • System Administrator passwords are minimum of 16 characters long • Passwords must contain a combination of numbers, 	<p>No Relevant Exceptions Noted</p>

		<p>uppercase letters, and lowercase letters</p> <ul style="list-style-type: none"> • The previous four passwords cannot be re-used • Passwords are updated every 90 days <p>Observed password settings in Backoffice and verified that the previous four passwords are remembered and cannot be re-used, and passwords must contain at least seven characters</p>	
CC6.2.5	Sessions are configured to timeout following a period of inactivity.	<p>Observed Microsoft Intune and Mosyle policies applied to all Windows and MacOS devices and verified that the screensaver locks after 10 minutes of inactivity, and a five-second grace period is applied within which the user will not be required to enter their password</p> <p>Observed that the timeout policy is enforced on end-user devices and verified that the policies are enforced</p>	No Relevant Exceptions Noted
CC6.2.6	Accounts are configured to lock for 30 minutes following six invalid login attempts.	<p>Interviewed the Manager of Security and IT Compliance and determined that user accounts are locked out after six invalid login attempts and for a duration of 30 minutes</p> <p>Observed Azure Active Directory lockout settings and verified that accounts are locked out for 30 minutes after six invalid login attempts</p>	No Relevant Exceptions Noted
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
CC6.3.1	The organization has a process for temporarily assigning elevated access to users following administrator approval.	<p>Reviewed the Information Security Policies and Procedures and verified that System Group approves access authorization based on an employee's job classification and function; a member of the Systems Group must review the Access Authorization Form to assure proper separation of duties; and contractor accounts require</p>	No Relevant Exceptions Noted

		<p>Systems Group approval and automatically expire at the end of the contract</p> <p>Observed that no users have permanent, read-write administrative access to the AWS Console and verified that when a PayByPhone employee needs elevated access to the AWS Console, they log into Bifrost and request elevated access, including with a time limit; another administrator on the approval list must approve the request, after which the requestor is granted elevated access to the AWS Console; when the time limit has expired, the requestor's access is automatically demoted to the prior access level; this is referred to as firefighter access, which is an example of just-in-time access management</p>	
CC6.3.2	Access is revoked for terminated employees, and the organization has a process for removing inactive accounts.	<p>Reviewed the Information Security Policies and Procedures and verified that access is revoked immediately for terminated, transferred, or unnecessary users, and user IDs are disabled after 90 days of inactivity and purged after an additional 30 days</p> <p>Observed offboarding records for a sample of terminated users (9 of 93) and verified that the employees were removed from all relevant systems, including BambooHR, Azure Active Directory, and Backoffice</p>	No Relevant Exceptions Noted
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	The organization implements mobile device management (MDM) processes to ensure that remote users have their devices protected.	Reviewed the Mobile Device Management Policy within the Information Security Policies and Procedures and verified that all company end-user devices are required to use desktop firewalls and connect using Zero Trust Network Access (ZTNA) solutions provided by the company, and the policy includes requirements for personal firewalls and use of the Zscaler Zero Trust Network	No Relevant Exceptions Noted

		<p>Access solution for remote access to company applications</p> <p>Interviewed the Manager of Security and IT Compliance and CISO & Senior Director of Reliability and determined that an inventory of company assets is maintained; all end-user devices are managed through MDM platforms as follows:</p> <ul style="list-style-type: none"> • Windows devices: Microsoft Intune • MacOS devices: Mosyle Enhanced Apple Device Management <p>Observed use of Intune (Windows) and Mosyle (MacOS) MDM platforms and verified that they are used to manage configurations for end-user devices</p> <p>Observed that PayByPhone has implemented end-user device safeguards and verified that each employee-assigned device presents its own security perimeter; critical elements of these end-point controls include:</p> <ul style="list-style-type: none"> • Centrally managed MDM using Microsoft Intune for Windows devices and Mosyle for MacOS • ZTNA using Zscaler • Centralized identity management using Azure Active Directory 	
CC6.4.2	AWS is responsible for protecting the data it houses on behalf of PayByPhone.	Observed that the organization obtained a SOC 2 audit report for AWS and verified that all critical systems and applications are located in AWS, which is responsible for physically protecting the data it holds; interested parties should review the subservice organization’s audit report	No Relevant Exceptions Noted
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.		

<p>CC6.5.1</p>	<p>The organization has a process for physically destroying assets and data.</p>	<p>Reviewed the Disposal Policy and verified that the following are enforced:</p> <ul style="list-style-type: none"> • Hard disks are sanitized using s National Institute of Standards and Technology (NIST) 800-88 standard degauss or crosscut shred to, or by penetrating the disk platters with one or more half inch holes drilled though them • Floppy disks are disintegrated, incinerated, pulverized, crosscut shred, or melted • Tape media are degaussed, crosscut shred, incinerated, pulverized, or melted • USB thumb drives, smart cards, and digital media are incinerated, pulverize, or melted • Optical disks (CDs and DVDs) are destroyed, incinerated, pulverized, crosscut shred, or melted • Before computer or communications equipment can be sent to a vendor for trade-in, servicing or disposal, all cardholder data must be destroyed or removed according to the approved methods • Removable computer storage media such as floppy, optical disks, or magnetic tapes may not be donated to charity or otherwise recycled • Outsourced destruction of media containing cardholder data must use a bonded disposal vendor that provides a Certificate of Destruction <p>Observed a completed Certificate of Destruction from DataKnox.io and verified that data was destroyed in accordance with NIST 800-53</p> <p>Observed a completed Certificate of Destruction from Infoshred and</p>	<p>No Relevant Exceptions Noted</p>
----------------	--	--	-------------------------------------

		verified that third parties are used to destroy data	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	Source code is reviewed prior to each change and is stored in GitLab and GitHub.	<p>Reviewed the Technical Standards and Policies documentation and verified that source code is stored in GitLab and GitHub, which uses Active Directory for authentication and authorization</p> <p>Reviewed the Code Review document and verified that the following are addressed:</p> <ul style="list-style-type: none"> • Code reviews are required for every code change • Reviewers must confirm that the reviewed code is free from security defects • A GitLab merge request is required for each code review • Merge requests should have at least one reviewer • For services deployed in the cardholder data environment, a Security Review confirmation is needed from at least one reviewer • Tickets are reviewed before deployments can be approved <p>Interviewed the Manager of Security and IT Compliance and CISO & Senior Director of Reliability and determined that the Terraform code is maintained in PayByPhone’s GitLab source code management repositories; developers have access to the source code repository (GitLab and GitHub)</p> <p>Observed that source code is stored in GitLab and GitHub and verified that authentication and authorization is managed using Active Directory</p> <p>Observed the use of GitLab and verified that Terraform is used to manage source code</p>	No Relevant Exceptions Noted

<p>CC6.6.2</p>	<p>The organization has a process for encrypting passwords during transmission and storage.</p>	<p>Observed the Backoffice password hash settings and verified that the Backoffice portal uses bcrypt for password hashing</p> <p>Observed that PayByPhone uses a cloud-based solution called Microsoft Azure Active Directory for authentication and verified that Microsoft handles the transmission of these passwords</p> <p>Observed access to infrastructure components and verified that access is provided through Azure Active Directory-integrated single sign-on</p> <p>Observed Azure Active Directory authentications and verified that they occur using Transport Layer Security (TLS) encrypted sessions under Microsoft management</p>	<p>No Relevant Exceptions Noted</p>
<p>CC6.6.3</p>	<p>Multi-factor authentication (MFA) is used for remote access to the organization’s corporate networks.</p>	<p>Reviewed Information Security Policies and Procedures (dated July 11, 2023) and verified that critical systems with access to the cardholder data environment should have two-factor authentication</p> <p>Interviewed the Information Security Lead and determined that the organization has implemented two distinct Azure Active Directory conditional access policies; the policies necessitate the use of MFA during login attempts, reinforcing the authentication process with an additional layer of identity verification</p> <p>Observed the use of Microsoft Authentication and verified that it is used for the MFA solution</p> <p>Observed the use of Zscaler to provide remote network access to the in-scope AWS accounts and virtual private clouds (VPCs) and verified that Zscaler authentication is integrated with Azure Active Directory, which</p>	<p>No Relevant Exceptions Noted</p>

		<p>requires MFA for all authentication requests regardless of application</p> <p>Observed that all accounts require the use of MFA and verified that MFA is implemented in Azure Active Directory; two Azure Active Directory conditional access policies have been implemented regarding MFA:</p> <ul style="list-style-type: none"> • “RequireMFA-MSAuth,” is designed for all users across the organization; this policy necessitates the use of MFA during login attempts for access to any PayByPhone Azure Active Directory-integrated application • “1 day sign-in frequency for admins,” specifically targets administrative users within the system; this policy mandates that administrators not only provide their password but also undergo MFA verification daily 	
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.		
CC6.7.1	<p>Sensitive data is secured any time it must be transmitted or received via open, public networks.</p>	<p>Interviewed the Manager of Security and IT Compliance and determined that all databases are encrypted by default by AWS Guardrails</p> <p>Observed cipher suite components and verified that they provide strong security</p> <p>Observed cryptography configurations for application programming interface (APIs) and application and verified that the configurations only receive traffic on TLS ports (TCP/443) in communication between all system components, and that TLS 1.2 is supported, and that strong cipher suite selections are supported including:</p> <ul style="list-style-type: none"> • Key exchanges supporting perfect forward secrecy with key lengths of 2048+ (FFC) and 256+ (elliptic curve) 	<p>No Relevant Exceptions Noted</p>

		<ul style="list-style-type: none"> • RSA host authentication with key lengths of 2048+ • AES128, AES256 and ChaCha20 bulk encryption SHA256 or stronger MAC <p>Observed that HTTP Strict Transport Security (HSTS) is required for all communications and verified that communication is delivered to all browsers that attempt to connect on HTTP</p> <p>Observed the encryption of sensitive data at rest and verified that encryption of PII is accomplished through AWS RDS-based encryption using an encryption key managed in AWS Key Management Service (KMS); encryption of cardholder data (CHD) is performed by the application using a custom-built application component that uses AWS-provided software development kits (SDKs) to interface with AWS KMS; and each data element is encrypted its own KMS-managed encryption key and stored in the database as encrypted content</p> <p>Observed encryption of data in transit and verified that all web application user interfaces and application programming interfaces use HTTPS based on TLS 1.2 and strong cipher suites</p>	
CC6.7.2	The organization uses AWS and Terraform to manage encryption keys.	<p>Reviewed the Cardholder Data Encryption Policy (dated August 17, 2023) and verified the following:</p> <ul style="list-style-type: none"> • Key management for cardholder data encryption keys is completed through Terraform in the terraform-encryption-keys-live repository • Access to encryption keys is managed by submitting a ticket to the Security and Compliance Service Desk • PII data is encrypted using AWS-provided capabilities for database 	No Relevant Exceptions Noted

		<p>encryption through the RDS service</p> <ul style="list-style-type: none"> • Encryption keys are managed through the AWS KMS <p>Interviewed the Manager of Security and IT Compliance and determined that AWS is responsible for key management</p> <p>Observed the use of AWS KMS and verified that it is used manage all encryption keys for sensitive data at rest</p> <p>Observed that encryption keys are retained in an AWS account and verified that it provides additional protection for KMS-related functions to restrict team member access unless a specific need exists to interact with KMS</p> <p>Observed the use of key management and verified that all key-encrypting keys are retained in AWS KMS, all data-encrypting keys are generated by AWS KMS, key-encrypting keys are automatically rotated on an annual basis, and encryption keys are retained in an isolated AWS account to provide additional access control for team members that can interact with the KMS</p> <p>Observed the effect of encryption on application data stored in DynamoDB and verified that the encrypted data is written to the database along with the necessary “encryption context” data for KMS to provide the plaintext key for future decryption operations</p> <p>Observed all other sensitive data is encrypted by AWS RDS-provided encryption features</p> <p>Observed RDS configurations and verified that encryption is enabled for</p>	
--	--	---	--

		each database instance that contains PII or other sensitive data	
CC6.7.3	The organization’s development, integration, consolidation, and production environments are unique environments that are logically separated, and the separation of duties are enforced throughout application development.	<p>Reviewed the Tenant Environments document and verified that the following are addressed:</p> <ul style="list-style-type: none"> • PayByPhone uses four environments as part of its SDLC: development, integration, consolidation, and production • Each environment is completely isolated and there is no connectivity between environments • Lowest level environments (development and integration) do not have outbound internet connectivity • Services in development and integration are not reachable from the internet without proper authentication • Development is unstable and meant to be used for experimentation • Consolidation access mimic the production environment in terms of network flow, access, IAM roles, and whitelisted AWS services <p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> • Personnel may be granted role-based access to the pre-production environments in order for users to perform job duties; however, access to production environments is only granted on a just-in-time, time-limited basis with explicit approval using the firefighter access request process • Tasks related to coding, testing, and maintaining the production environment are separated and the company establishes a barrier between development project teams and the production environment 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • User stories are written and security requirements are established by the product management team; the development team and solutions architect shape the security requirements during the story-writing process • The production personnel do not write code and test software, but they maintain the production environment and make sure there is a barrier between project teams and the production environment <p>Observed a screenshot showing personnel access to the pre-production environments for the multi-domain tenant and verified that there is no nominal access to the production environment</p> <p>Observed separation of production and non-production environments (development, integration-testing, and consolidation) through distinct AWS accounts and verified that there exist no network connections between prod and non-prod accounts and resources</p>	
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.		
CC6.8.1	Antivirus is installed on all removable media and end-user endpoints to detect and prevent the intrusion of malicious software.	<p>Interviewed the Manager of Security and IT Compliance and determined that antivirus is used on all end-user endpoints; as all production application workloads are based on Docker containers, antivirus is managed by AWS on the underlying infrastructure</p> <p>Observed use of Microsoft Defender antivirus as managed through Microsoft Intune and verified that Intune enforces the use of Defender for all Intune-managed devices, including both Windows and MacOS operating systems</p>	No Relevant Exceptions Noted

		Observed the use of Microsoft Defender antivirus and verified that Microsoft Defender is configured to scan all removable media for potential malware, and it is configured to receive daily updates	
--	--	--	--

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories

System Operations

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
CC7.1.1	<p>Web application testing and sprints are used to ensure that applications are not susceptible to common vulnerabilities.</p>	<p>Reviewed the Vulnerability Management Policy within the Information Security Policies and Procedures and verified the following:</p> <ul style="list-style-type: none"> • Public-facing web applications are required to be reviewed, and that all vulnerabilities identified are required to be corrected; the application is to be re-evaluated after the corrections have been made • The organization implements application vulnerability management practices to identify and prevent common web application vulnerabilities <p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> • Starting with writing user stories, security requirements are established by the product management team • As part of writing user stories, the development team and the solutions architect are involved in shaping the security requirements • Once the stories are planned into a sprint, the development team implements and tests the story • PayByPhone follows a test-driven development (TDD) approach, ensuring that if the security requirement can be proven via a unit or integration test it will be, even before the implementation code change is made • If it cannot be tested with a unit or integration test, then it is tested 	Exception Noted

		<p>manually, potentially with security testing tools, before it is marked as complete</p> <ul style="list-style-type: none"> • Test-driven development is practiced, and regression tests are used to identify and fix security bugs • Dynamic analysis is performed on UI-based endpoints using the Tenable web application scanner <p>Observed reports from JFrog and verified that JFrog scanning is built into the continuous integration and continuous delivery (CI/CD) pipeline; the organization uses JFrog for scanning containers to be deployed in pre-production and production environments and also run Tenable scans on the production, development, quality assurance (QA), and test environments</p> <p>Observed Tenable.io vulnerability scans completed against all public-facing API and UI endpoints and verified that scans are completed approximately every 90 days</p> <p><i>Exception: As determined through a penetration test of the PayByPhone applications, the Backoffice application was vulnerable to a URL redirection weakness, which allowed bad actors to use the application to redirect users to websites of the actor's choosing. The auditor observed updated penetration testing results (October 2023) to confirm that each of these items were remedied.</i></p>	
CC7.1.2	Internal and external scans are conducted on a regular basis to identify potential vulnerabilities, which are prioritized and remediated based on severity.	<p>Reviewed the Vulnerability Management Policy within the Information Security Policies and Procedures and verified the following:</p> <ul style="list-style-type: none"> • The Systems Group is responsible for conducting internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system 	No Relevant Exceptions Noted

		<p>component installations, changes in network topology, firewall rule modifications, product upgrades), and the process includes identifying any unauthorized wireless devices on the network</p> <ul style="list-style-type: none"> • When internal vulnerability scans identify high-risk vulnerabilities, the issues must be remediated and rescans must be performed after remediation to verify that the high-risk vulnerabilities are resolved • Additional external vulnerability scans must be performed by a scan vendor qualified by the payment card industry at least quarterly; the results of each scan must satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities) • When external vulnerability scans identify vulnerabilities with a CVSS score of 4.0 or higher, the issues must be remediated and rescans must be performed after remediation to verify that the vulnerabilities are resolved <p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> • Docker containers are used throughout the production applications, and AWS ECR Container Image Scanning is performed when a new image is pushed to the repository and continuously on all images uploaded in the prior 30 days • Scans are performed on end-user devices using Microsoft Defender, and these scans are performed weekly against all user endpoints • Alerts are delivered to a Slack channel shared with operations teams and that vulnerability scans are conducted as follows 	
--	--	---	--

		<p>Observed ECR image scanning configuration and verified that it is enabled and actively identifies new vulnerabilities in existing images</p> <p>Observed the use of agent-based Microsoft Defender and verified that Microsoft Defender is used to conduct scanning on end-user devices</p> <p>Observed external vulnerability scans and verified that they are completed on a weekly basis</p>	
CC7.1.3	<p>The organization conducts application and network layer penetration testing annually and following significant changes to the network in order to identify and remediate weaknesses.</p>	<p>Reviewed the Vulnerability Management Policy within the Information Security Policies and Procedures and verified penetration tests at both the application and network layer must be performed annually or after any significant change in the network</p> <p>Interviewed the Information Security Lead and determined that penetration tests at both the application and network layer must be performed annually or after any significant change in the network; PayByPhone uses a security company who is qualified to perform internal as well as external penetration testing</p> <p>Observed the external application and network penetration test report (dated August 2023) and verified that the penetration tests cover external, internet-accessible systems and applications were completed by an external company specializing in penetration testing services</p> <p>Observed that penetration testing is performed by a third party specializing in penetration testing services and verified that penetration tests evaluate the security of infrastructure, and both user and API interfaces; exploitable vulnerabilities are identified,</p>	<p>No Relevant Exceptions Noted</p>

		remediated, and retested to verify effective remediation	
		Observed penetration testing results and verified that that testing was performed by Mirai Security, penetration tests include infrastructure and application components, and exploitable vulnerabilities were retested after remediation	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity’s ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
CC7.2.1	Network monitoring and logging tools are installed to capture security events.	<p>Interviewed the Manager of Security and IT Compliance, the CISO & Senior Director of Reliability, and the Software Architect and determined the following:</p> <ul style="list-style-type: none"> • Security-related event logs are captured by the AWS, Bifrost, and Google Apigee cloud platforms • All actions taken against AWS-based assets are captured via AWS CloudTrail, written to a dedicated S3 bucket, and reviewed by CloudGuard • Logs are retained for at least one year to support forensic reviews in the case of a security incident <p>Observed use of AWS CloudTrail, CloudGuard, Slack, and PagerDuty and verified that they are used to collect, review, analyze, and provide relevant notifications pertaining to security events within the production infrastructure</p> <p>Observed Jira tickets from operational errors experienced in the production environment and verified tickets are used in response to application failures, which led to diminished performance, including failed payment processing functions</p>	No Relevant Exceptions Noted

		Observed the use of Datadog and verified that it is used to monitor various services within the production application and to notify operations staff via PagerDuty	
CC7.2.2	Intrusion detection and prevention tools are in place to detect anomalies and alerts are sent to personnel for remediation.	<p>Reviewed the Vulnerability Management Policy within the Information Security Policies and Procedures and verified that networks and systems that fall under payment card system scope must also be monitored by an intrusion detection or prevention system that alerts personnel of potential compromises</p> <p>Observed that GuardDuty is enabled on select AWS accounts and verified that the GuardDuty for the accounts are centrally managed by Managed Private Servers (MPS), who notifies PayByPhone if there are findings</p>	No Relevant Exceptions Noted
CC7.2.3	Logs are reviewed as part of daily security activities in order to detect and remediate suspicious activity.	<p>Interviewed the Manager of Security and IT Compliance, the Information Security Lead, and the Information Security Analyst and determined the following:</p> <ul style="list-style-type: none"> • Security logs are reviewed by automated log review tools to detect and notify operations personnel of potential security incidents • Check Point CloudGuard provides ongoing review and analysis of CloudTrail and other audit logs and provides notification through PagerDuty when suspicious activity is detected • The Security team performs a daily check of CloudGuard <p>Observed CloudTrail and CloudGuard configurations and verified that all relevant security events are reviewed daily</p> <p>Observed use of Slack channels, including the Sys911 channel, and verified that it is used to notify</p>	No Relevant Exceptions Noted

		operations personnel of security anomalies, that each notification is presented as a thread in Slack, and that follow-up was performed by relevant personnel and documented in each threaded item	
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
CC7.3.1	Security incidents are analyzed to determine appropriate remediation and prevention activities.	<p>Reviewed the Incident Response and verified that the following are addressed:</p> <ul style="list-style-type: none"> • Incident process • Post-incident process • Major incident process • Security incident process <p>Reviewed the Sys911 Incident Response and Resolution Procedure and verified that it includes a detailed process flow chart to follow in the event of a production alert</p> <p>Reviewed the Security Incident Response Policy and verified that it outlines requirements, policy statements, and initial process for reporting and responding to security events</p> <p>Interviewed the Manager of Security and IT Compliance and the CISO & Senior Director of Reliability and determined the following regarding availability and security incidents:</p> <ul style="list-style-type: none"> • If the incident is a single domain, then the incident is managed by the Service Platform team • If the incident is a multi-domain, then an incident commander is assigned, who coordinates the incident and updates the status page • As needed to resolve the incident, the incident command brings in additional resources and manages both internal and external communications 	No Relevant Exceptions Noted

		<p>Observed Jira ticket for a recent incident regarding the unexpected discovery of CHD in an application log and verified the following:</p> <ul style="list-style-type: none"> • Communication strategies, roles, and responsibilities were implemented in the related Slack security alerts channel • The root cause of the incident was identified as .Net application code that added ApplePay device primary account numbers (DPANs) to Datadog application logs • .Net coding changes were observed to be implemented through an associated development ticket (UB-3640) • Data clean-up was observed in engineering tickets associated with the master ticket 	
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
CC7.4.1	<p>Incident response policies and procedures have been formally documented and implemented to define incident identification, reporting, containment, and remediation processes.</p>	<p>Reviewed the Incident Response and verified that the following are addressed:</p> <ul style="list-style-type: none"> • Incident process • Post-incident process • Major incident process • Security incident process <p>Reviewed the Sys911 Incident Response and Resolution Procedure and verified that it includes a detailed process flow chart to follow in the event of a production alert</p> <p>Reviewed the Security Incident Response Policy and verified that it outlines requirements, policy statements, and initial process for reporting and responding to security events</p> <p>Interviewed the Manager of Security and IT Compliance and the CISO & Senior Director of Reliability and determined and determined the</p>	<p>No Relevant Exceptions Noted</p>

		<p>following regarding availability and security incidents:</p> <ul style="list-style-type: none"> • If the incident is a single domain, then the incident is managed by the Service Platform team • If the incident is a multi-domain, then an incident commander is assigned, who coordinates the incident and updates the status page • As needed to resolve the incident, the incident command brings in additional resources and manages both internal and external communications <p>Observed Jira ticket for a recent incident regarding the unexpected discovery of CHD in an application log and verified the following:</p> <ul style="list-style-type: none"> • Communication strategies, roles, and responsibilities were implemented in the related Slack security alerts channel • The root cause of the incident was identified as .Net application code that added ApplePay DPANs to Datadog application logs • .Net coding changes were observed to be implemented through an associated development ticket (UB-3640) • Data clean-up was observed in engineering tickets associated with the master ticket 	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	<p>Outside sources are reviewed to identify patches and new vulnerabilities that could impact the organization’s networks and systems, and patches are installed based on the criticality of the vulnerability.</p>	<p>Reviewed the Vulnerability Management Policy within the Information Security Policies and Procedures and verified the following:</p> <ul style="list-style-type: none"> • All security patches, hot-fixes, and service packs identified by the Systems Group or the System Administrator must be installed on applicable systems within 30 days of vendor release and in 	<p>No Relevant Exceptions Noted</p>

		<p>accordance with change management processes</p> <ul style="list-style-type: none"> • Critical and high-ranking vulnerabilities are patched within 30 days • Medium and low vulnerabilities are patched within three months <p>Interviewed the Manager of Security and IT Compliance and the CISO & Senior Director of Reliability and determined the following:</p> <ul style="list-style-type: none"> • Members of the Systems Group must be informed of information security issues and vulnerabilities applicable to PayByPhone computing systems • When security issues are identified, the Systems Group is responsible for notifying appropriate personnel, including System Administrators • The primary method for identifying new threats is through vendor and security-specific internet mailing lists • The organization subscribes to NVD, Microsoft, AWS, and as well as other vendor lists applicable to PayByPhone-specific software packages and systems • New vulnerabilities are communicated through Slack and evaluated for impact on PayByPhone technologies • New security vulnerabilities are required to be monitored and are assigned a risk ranking <p>Observed use of Slack and verified that it is used to receive and triage new vulnerabilities</p>	
CC7.5.2	The organization incorporates lessons learned from incident response activities into the incident response policies and procedures.	<p>Reviewed the Incident Response and verified that the post-incident process is addressed</p> <p>Interviewed the Manager of Security and IT Compliance and the CISO &</p>	No Relevant Exceptions Noted

		<p>Senior Director of Reliability and determined that once the incident is resolved, the team conducts a post-mortem exercise to identify the cause and improvements to prevent a recurrence</p> <p>Observed Jira ticket for a recent incident regarding the unexpected discovery of CHD in an application log and verified the following:</p> <ul style="list-style-type: none"> • Communication strategies, roles, and responsibilities were implemented in the related Slack security alerts channel • The root cause of the incident was identified as .Net application code that added ApplePay DPANs to Datadog application logs • .Net coding changes were observed to be implemented through an associated development ticket (UB-3640) • Data clean-up was observed in engineering tickets associated with the master ticket <p>Observed the master Security Incident Response ticket and verified that lessons learned from the incident are documented</p>	
--	--	---	--

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories

Change Management

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.1	<p>Formal configuration standards are maintained for all systems in use within the environment, and systems are required to be configured appropriately prior to promotion to the production networks.</p>	<p>Reviewed the Information Security Policies and Procedures document (dated August 7, 2023) and verified that all servers and network devices on PayByPhone networks, whether managed by employees or by third parties, are built and deployed in accordance with a system configuration policy; the following system build and deployment guidelines are enforced:</p> <ul style="list-style-type: none"> • Maintain a System Configuration Record for each deployed system, updating it with any modifications • Enforce file integrity monitoring (FIM) software for systems handling cardholder data • Install antivirus software on operating systems • Log, monitor, and review changes on critical systems • Update affected consoles and remove from Nessus Policy scan when deactivating a system <p>Interviewed the Manager of Security and IT Compliance and CISO & Senior Director of Reliability and determined the following:</p> <ul style="list-style-type: none"> • All production application assets are provided as Docker containers running under AWS Elastic Container Service (ECS) • Some application containers are based on Alpine Linux and others are based on Microsoft Windows • In all cases, however, AWS resources are configured using infrastructure-as-code practices based Terraform 	<p>No Relevant Exceptions Noted</p>

		<ul style="list-style-type: none"> • AWS-based components, including ECS clusters, VPC networks, cloud firewalls, S3 buckets, and KMS are securely configured following industry best practices based on AWS and Center for Internet Security (CIS) guidance <p>Observed the use of Terraform and verified that it is used to configure AWS infrastructure and services</p> <p>Observed Dockerfile hardening and verified that it is consistent with CIS Docker benchmark recommendations</p>	
CC8.1.2	System configurations are reviewed on a daily basis.	<p>Interviewed the Manager of Security and IT Compliance and determined that daily reviews are performed by the Security team to confirm that critical security configurations remain in place</p> <p>Observed the IT Daily Security Check Log (dated September 2023) and verified that configurations are checked and reviewed daily on the following critical items:</p> <ul style="list-style-type: none"> • Email system • Microsoft Defender • Datadog – SQL Injection & SMS dashboard • CloudGuard • Microsoft Purview • AWS Macie 	No Relevant Exceptions Noted
CC8.1.3	The organization maintains formally documented roles and responsibilities for personnel involved in maintaining system configuration standards.	<p>Reviewed the Information Security Policies and Procedures document (dated August 7, 2023) and verified that the following personnel are responsible for system configuration standards:</p> <ul style="list-style-type: none"> • CTO or designated officer is responsible for coordinating and overseeing PayByPhone wide compliance with policies and procedures • The Systems Group is dedicated to security planning, education, and awareness • Cloud Platform Infrastructure team manages the PayByPhone 	No Relevant Exceptions Noted

		<p>solutions production and development environments</p> <ul style="list-style-type: none"> Corporate IT Team is responsible for corporate user environments and services 	
CC8.1.4	<p>Change management policies and procedures are implemented and require the documentation of approval by authorized parties and the testing of functionality prior to implementation.</p>	<p>Reviewed the change management process within the Information Security Policies and Procedures (dated September 4, 2023) and verified the following:</p> <ul style="list-style-type: none"> All proposed changes to PayByPhone network devices, systems, and application configurations must follow this policy The party responsible for implementing the change is required to complete and submit the appropriate electronic change request to the Systems Group’s manager or the manager of the Research and Development team Changes must receive management approval by the CTO, designated officer, or manager assigning the task Changes must be tested on a QA or test network that is isolated from the production Test plan should be followed to ensure there are no adverse effects If any discrepancies between expected and actual results that impact the network, systems, applications, business requirements, or support procedures occur, the documented back out procedures are immediately implemented <p>Interviewed the Manager of Security and IT Compliance and CISO & Senior Director of Reliability and determined the following:</p> <ul style="list-style-type: none"> Change management practices are implemented to ensure that changes to the system are controlled 	<p>No Relevant Exceptions Noted</p>

		<ul style="list-style-type: none"> • All changes to both infrastructure and applications are managed through a single process that is implemented through Jira tickets • Changes are tested in pre-production environments consisting of development, integration, and consolidation prior to implementation in production <p>Observed the use of Jira tickets for tracking all changes and verified that Jira tickets capture the following information:</p> <ul style="list-style-type: none"> • Links to related pull and merge requests where application code review results and other necessary application details are captured • A description of the change and associated risks • Necessary approvals prior to implementing the changes • Testing results, including both manual and CI-driven testing • Backout plans in the event the change is unsuccessful <p>Observed that all changes are implemented as infrastructure-as-code and verified that the change followed the standard deployment pipeline, including testing in pre-production environments</p>	
CC8.1.5	Code reviews are conducted prior to changes being implemented.	<p>Reviewed the Code Reviews document and verified that the code review process is documented on Confluence; code reviews are required for every single code change; and reviewers must acknowledge in the review that the reviewed code is free from security defects before the review can be passed</p> <p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> • Code reviews are necessary to allow a change to be made in production 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Code reviews are completed by an individual (one or more developers and occasionally QAs) who did not write the code, and their review comment must indicate that they did a PCI or security assessment of the change • If an issue is found, then the original coder addresses the issue, puts it back through QA, and completes the code review process before it can be deployed to production • Once deployed, it is smoke tested and, if deemed necessary for the change, further security testing with security testing tools is used in production • OWASP guidelines are reviewed and complied with during code reviews <p>Observed Jira tickets and verified that each deployment in Jira has a linked team ticket that contains the actual deployment branch</p>	
CC8.1.6	The organization maintains software development checklists to ensure the security during application development.	<p>Reviewed the Production Readiness Checklist and the Design Review Checklist and verified that it the following security, compliance, and privacy standards are addressed:</p> <ul style="list-style-type: none"> • Code deploys are automated and run from a server or platform, not from developer machines • Deploys are zero-downtime, ensuring the availability of the service • Automated rollback is possible within five minutes or less • Terraform is used for deploying infrastructure • One-time database changes are source-controlled, and database schema changes are automated for non-legacy databases • Security review is performed by PayByPhone’s Security team, including risk assessment and penetration testing 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Code is internally reviewed for security with respect to the OWASP Top 10 vulnerabilities • Third-party library versions used have no known vulnerabilities, and licensing compliance is checked • APIs accessed by consumer apps or the back office use appropriate authentication mechanisms • Service logging is in place, excluding personally identifiable information (PII) and sensitive data • PII is hashed or encrypted using approved mechanisms and not written to logs • GDPR “right to be forgotten” is supported, allowing the removal or anonymization of personal data <p>Interviewed the Manager of Security and IT Compliance and determined that project management methodologies like Scrum, Kanban, and Scrumban are used, and work progress is tracked in Jira</p> <p>Interviewed the Manager of Security and IT Compliance and CISO & Senior Director of Reliability and determined that pipeline automation through GitLab CI is used to reduce the opportunities for human error in managing changes; once approved for introduction in the various operating environments, GitLab CI performs the deployment and measures the results with pre-defined tests to ensure that common errors are caught and corrected prior to production deployments; OWASP and general security best practices are always taken into account and are tracked in the Crucible code reviews</p> <p>Observed Jira tickets and verified that each deployment in Jira has a linked team ticket that contains the actual deployment branch</p>	
--	--	---	--

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories

Risk Mitigation

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	<p>Risk mitigation activities are identified based on the results of the annual risk assessment and are selected by executive management.</p>	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that the Systems Group and ITOPS team does the following:</p> <ul style="list-style-type: none"> • Conducts an annual formal risk assessments to identify new threats and vulnerabilities • Perform risk assessments when significant changes occur in the environment • Informs the company about information security issues and vulnerabilities • Monitors and identifies new security vulnerabilities and assigns risk rankings to them • Uses reputable outside sources for vulnerability information • Subscribes to vendor and security-specific internet mailing lists for threat identification • Maintains updates and patches for operating systems and applications <p>Interviewed the Manager of Security and IT Compliance and determined that the Compliance team reviews all risks monthly</p> <p>Interviewed the Manager of Security and Compliance and determined the following:</p> <ul style="list-style-type: none"> • At least annually, the organization coordinates a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks 	<p>No Relevant Exceptions Noted</p>

		<ul style="list-style-type: none"> Security risk assessments are reported and are shared with the Board on a quarterly basis <p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p>	
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Due diligence is performed prior to the selection of new vendors or service providers.	<p>Interviewed the Manager of Security and IT Compliance and determined that PayByPhone’s vendor due diligence procedures consists of the following:</p> <ul style="list-style-type: none"> PayByPhone engages with a vendor for proof of concept (POC) early in the process During POC, PayByPhone acquires compliance documentation, such as ISO 27000, SOC 2, and PCI AOC If the vendor cannot provide appropriate audit reports, PayByPhone engages in a vendor risk assessment; the process is ad-hoc and tailored to the individual vendor Legal is engaged for a contract once the POC is successful <p>Observed Zscaler documentation and verified that Zscaler underwent a full review before being accepted as a vendor</p>	No Relevant Exceptions Noted
CC9.2.2	Vendors and service providers are required to review and sign a non-disclosure agreement (NDA) and contract prior to sharing information with the organization.	<p>Interviewed the Manager of Security and IT Compliance and determined that PayByPhone signs NDAs with vendors prior to sharing any confidential information</p> <p>Observed the PayByPhone NDA template and verified that it is a mutual NDA that binds each receiving party to hold confidential information as disclosed by the disclosing party, and the agreement requires that the receiving party protects the information with no less than “reasonable care” and consistent with</p>	No Relevant Exceptions Noted

		<p>the measures it would take to protect its own confidential information</p> <p>Observed completed contracts and verified that contracts are established between PayByPhone and their subservice organizations, where the subservice organizations commit to providing data security controls relevant to the services they provide</p>	
CC9.2.3	<p>Audit reports are required to be collected from vendors annually to ensure their continued compliance.</p>	<p>Interviewed the Manager of Security and IT Compliance and determined that the organization has a process to manage vendors; the organization annually reviews all critical vendors and gathers the most recent audit reports, such as ISO 27000, SOC 2, and PCI DSS; when reviewing the SOC 2 exceptions, reasonable controls, and the opinion are reviewed</p> <p>Observed that the organization obtained AOCs from AWS, Azure, and Google and verified that the reports were obtained to review the third parties' compliance standing</p> <p>Observed SOC review tickets and verified that SOC 2 reports are reviewed as part of the vendor monitoring process</p>	<p>No Relevant Exceptions Noted</p>

Additional Criteria for Availability			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
A1.1.1	Tools are installed to monitor systems to enable personnel to evaluate capacity and monitor system health.	<p>Interviewed the Manager of Security and IT Compliance, the CISO & Senior Director of Reliability, and the Software Architect and determined that application performance is monitored through Datadog, where numerous metrics are reviewed and analyzed, and when performance is outside of expectations, Datadog generates alerts to operations through both Slack channels and PagerDuty</p> <p>Observed use of Datadog to monitor application performance and verified that the dashboards monitor the following:</p> <ul style="list-style-type: none"> • Site Reliability – Mission Control • Payment Processor Business Dashboard • Corporate Accounts Dashboard • Log Management – Estimated Usage • Dialogue Flow API (Cloud Interactive Voice Response [IVR]) • Apigee Nginx Inbound Proxy • ECS Resource Consumption • Internal Parking API • AWS Oracle RDS Dashboard • Security Dashboard • Payment Processor Service • Business Operations (API Consumption) <p>Observed use of Slack and PagerDuty and verified that they are used to provide notifications to operations teams when parameters do not meet expectations</p>	No Relevant Exceptions Noted
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		

<p>A1.2.1</p>	<p>The organization has established tools and processes to ensure backups are consistently and securely completed.</p>	<p>Reviewed the Data Backup Policies and verified the following:</p> <ul style="list-style-type: none"> • Backups have deletion protection and remain available even if the associated AWS resources are deleted • In the backup solution, “mps-daily-backup-plan” provides daily backups for five weeks in the MPS Backup vault, “mps-weekly-backup-plan” offers weekly backups for three months in the MPS Backup vault, and “mps-monthly-backup-plan” allows monthly backups for three months in the MPS Backup vault • For staging environments, apply the “mps:business-continuity:backup-plan” tag to non-production environments • The supported services for the backup solution include Amazon Aurora clusters, Amazon EBS volumes, Amazon EC2 instances, Amazon DynamoDB tables, Amazon EFS file systems, Amazon FSx file systems, and Amazon RDS databases <p>Interviewed the Manager of Security and IT Compliance and the Information Security Lead and determined that all backups are performed through the AWS RDS-provided capabilities; backups are encrypted and stored by RDS and restore points for Oracle databases are available for one week; and AWS provides capabilities to perform a point-in-time restore to any point in time within the available backups window</p> <p>Observed RDS configurations and verified that Oracle instances are configured for multi-Azure availability, and encryption of both the instances and the backups</p>	<p>No Relevant Exceptions Noted</p>
---------------	--	---	-------------------------------------

		<p>Observed RDS Automated Backup configurations and verified that snapshots are taken daily, and that point-in-time restore allows restoration to any point within the available snapshots window</p> <p>Observed available snapshots and verified that databases can be restored to any point in time within the prior seven days</p> <p>Observed that RDS backups are managed entirely by AWS</p>	
A1.2.2	<p>Plans are in place to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.</p>	<p>Reviewed the Data Backup Policies and verified that the disaster recovery policy focuses on one-time recovery objectives in response to natural disasters, large-scale technical failures, or human threats such as attack or error</p> <p>Reviewed the Disaster Recovery Plan & Business Continuity Plan and verified the following attributes are addressed:</p> <ul style="list-style-type: none"> • The primary objective of this Disaster Recovery Plan is to ensure continual operations of identified critical business systems in the event of a disaster • Recovery and response capabilities are built around a tiered approach (Tier 0 through Tier 4) where Tier 0 services include core AWS capabilities and application infrastructure, progressing through the other tiers based on revenue and customer impact • List of critical components and software • Conditions for activating the plan • Awareness and education activities • The overall recovery time objective (RTO) is established at 24 hours and the recovery point objective (RPO) for parking- 	<p>No Relevant Exceptions Noted</p>

		<p>related services is documented as 15 minutes</p> <ul style="list-style-type: none"> • The plan defines the roles and responsibilities for personnel during a disaster, including the following: <ul style="list-style-type: none"> ○ Roles ○ Incident coordinator ○ Disaster Recovery team ○ Corporate IT Recovery team ○ Platform Recovery team ○ Service Recovery teams ○ Communication coordinator <p>Interviewed the Manager of Security and IT Compliance and determined that staff have access to all business operations services whole working remotely; all business are software as a service (SaaS) or cloud-based</p>	
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A1.3.1	The organization regularly tests backup restoration activities.	<p>Interviewed the Manager of Security and IT Compliance and the Information Security Lead and determined that backup restore operations are tested</p> <p>Observed a Jira ticket number and verified that the test conducted was used to confirm Backoffice-related databases and services are configured for high availability, and the outcome confirmed and documented at best high availability configuration above in Confluence or Jira assets for all related Backoffice service</p> <p>Observed a ticket that captured a test of Backoffice deletion and restoration of databases in CONS and verified that the test was completed and had a successful outcome and was well documented</p> <p>Observed a ticket that captured a test of a test to delete and restore platform RDS databases in CONS and verified that test procedures were well documented with lessons learned and</p>	No Relevant Exceptions Noted

		<p>follow-up questions for improvement next time</p> <p>Observed restoration test results and verified that the following databases are tested for restoration:</p> <ul style="list-style-type: none"> • RDS Oracle • RDS Postgres • RDS MySQL • Aurora DBs • Postgres • MySQL • DynamoDB 	
A1.3.2	The Disaster Recovery Plan & Business Continuity Plan is tested and updated annually.	<p>Reviewed the Disaster Recovery Plan & Business Continuity Plan (dated September 14, 2023) and verified that the plan is tested annually</p> <p>Interviewed the Manager of Security and IT Compliance and determined that the business continuity and disaster recovery plans must be reviewed and tested annually and are updated as needed based on the findings</p>	No Relevant Exceptions Noted

Additional Criteria for Confidentiality			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
C1.1.1	Data is classified into one of three defined categories: sensitive, private, and public.	<p>Reviewed the Data Classification & Guidance document and verified that the following categories are in place:</p> <ul style="list-style-type: none"> • Sensitive – Applies to less sensitive business information which is intended for use within PayByPhone; unauthorized disclosure could adversely impact the company, its stockholders, its business partners, and/or its customers; and examples of sensitive information include, internal market research, and audit reports • Private – Applies to personal information, which is intended for use within PayByPhone; unauthorized disclosure could adversely impact the company and/or its employees; and examples of private information include policies and procedures, procedure metrics, and intellectual property • Public – Applies to all other information which does not clearly fit into any of the aforementioned categories; unauthorized disclosure is not expected to seriously or adversely impact the company; and any release of this information must be authorized by PayByPhone Public Relations Department <p>Interviewed the Information Security Analyst and determined that all cardholder and PII data are considered confidential; unauthorized disclosure could seriously and adversely impact the company, stockholders, business partners, and/or its customers</p>	No Relevant Exceptions Noted
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		

<p>C1.2.1</p>	<p>The organization has a process for destroying and disposing of data and media when no longer needed.</p>	<p>Reviewed the Disposal Policy and verified that the following are enforced:</p> <ul style="list-style-type: none"> • All cardholder electronic or hardcopy data, when no longer needed for legal, regulatory, or business requirements, must be securely deleted from PayByPhone systems using company-approved method • A programmatic (automatic) process is executed when a customer enters a new credit card; the old credit card is removed and the new card inserted • Other applicable data stored in files and directories where the containing media is re-used must be deleted securely by a wiping utility approved by the Systems Group <p>Observed a completed Certificate of Destruction from DataKnox.io and verified that data was destroyed in accordance with NIST 800-53</p> <p>Observed a completed Certificate of Destruction from Infoshred and verified that third parties are used to destroy data</p>	<p>No Relevant Exceptions Noted</p>
---------------	---	---	-------------------------------------

Additional Criteria for Processing Integrity			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.		
PI1.1.1	The organization has tools in place to monitor services and projects.	<p>Observed the use of Datadog and verified that Datadog is used to monitor their services, providing metrics and dashboards accessible to both business and technical staff</p> <p>Observed the use of real-time monitoring of payment transactions and verified that alerts are triggered for a specified number of failures or declines over a specific timeframe</p> <p>Observed alerts are sent via Pager Duty to the on-call PayByPhone support personnel and verified that whoever receives the alert assesses and addresses the issue, often by disabling suspicious motorist accounts</p> <p>Observed Confluence and verified that project monitoring is facilitated through Confluence, and regular project updates are provided to the executive team</p> <p>Observed the use of the Payment Processor Runbook and verified that it is used diagnose and remediate various processing errors that can occur on the platform</p>	No Relevant Exceptions Noted
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.		
PI1.2.1	Checklists are used to ensure all new customers are onboarded and assigned access to online services.	<p>Interviewed the Manager of Security and IT Compliance and determined that a client implementation checklist is used to drive implementations for new customers</p> <p>Observed the Project Check List and verified that the includes details necessary for onboarding new customers</p>	No Relevant Exceptions Noted

		Observed the onboarding process for three new customers (parking authorities) and verified that project checklist spreadsheets are completed	
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity’s objectives.		
PI1.3.1	Logs capture relevant events and are protected against accidental file deletion.	<p>Reviewed the AWS Tagging Policy and verified that it contains AWS tagging policies for backups, including backup plan tag requirements</p> <p>Observed that all system infrastructure is implemented through AWS-provided technologies and verified that AWS CloudTrail logs are enabled and actively capturing relevant events to a dedicated AWS CloudTrail S3 bucket; the bucket is protected from accidental file deletion events and configured with a lifecycle policy to ensure retention of data</p>	No Relevant Exceptions Noted
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity’s objectives.		
PI1.4.1	Operational training materials are provided to clients that outline how to correctly use the Backoffice portal application.	<p>Interviewed the Manager of Security and IT Compliance and determined that PayByPhone provides a Portal User Guide to customers (parking authorities) that outlines how to use the Backoffice portal application</p> <p>Observed the 2023 Portal Users Guide and verified that the document is written for customers’ use of the Backoffice portal</p>	No Relevant Exceptions Noted
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity’s objectives.		
PI1.5.1	Data retention requirements are defined and implemented.	<p>Reviewed Information Security Policies and Procedures (dated July 11, 2023) and verified that the following data handling requirements are defined:</p> <ul style="list-style-type: none"> • Data retention • Data disposal • CHD retention and purging 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> ○ Stale CHD data is purged after 36 months ○ Expired CHD is purged after nine months <p>Interviewed the Manager of Security and IT Compliance and determined that when the PEER1 data center systems were decommissioned as part of the transition to a cloud-only application delivery model, the assets in the data center were physically destroyed by a third party</p> <p>Observed records for three recently deactivated customers (parking authorities) and verified evidence of decommissioning customer accounts</p>	
--	--	--	--



PayByPhone Technologies, Inc.

Type II System and Organization Controls Privacy Report (SOC 2 Privacy)

Report on a Service Organization's Description of Its System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Privacy Throughout the Period November 1, 2022, to October 31, 2023.



KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

KirkpatrickPrice.

innovation. integrity. delivered.

TABLE OF CONTENTS

SECTION I: ASSERTION OF PAYBYPHONE TECHNOLOGIES, INC. MANAGEMENT	1
Assertion of PayByPhone Technologies, Inc. Management.....	2
SECTION II: INDEPENDENT SERVICE AUDITOR’S REPORT	4
Independent Service Auditor’s Report	5
Scope	5
Service Organization’s Responsibilities	6
Service Auditor’s Responsibilities	6
Inherent Limitations	7
Description of Tests of Controls.....	7
Opinion	7
Restricted Use.....	8
SECTION III: PAYBYPHONE TECHNOLOGIES, INC.’S DESCRIPTION OF ITS PAYMENT PROCESSING SERVICES SYSTEM RELATED TO PRIVACY	9
Services Provided	10
Principal Service Commitments and System Requirements.....	12
Regulatory Commitments	12
Contractual Commitments.....	12
System Design.....	12
Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring	13
Control Environment Relevant to Privacy	13
Notice and Communication of Objectives Related to Privacy.....	13
Choice and Consent	13
Collection.....	14
Use, Retention, and Disposal	14
Access	15
Disclosure and Notification	15
Quality	16
Monitoring and Enforcement	17
Risk Assessment Process	17
Information and Communication Systems	17
Monitoring Controls.....	18
Changes to the System Related to Privacy During the Period	18
Complementary User-Entity Controls	20

SECTION IV: TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS 22

- Applicable Trust Services Criteria Relevant to Privacy 23
 - Privacy..... 23
 - Common Criteria Related to Security 23
 - Trust Services Criteria for the Privacy Category 25
 - P1.0 Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy... 25
 - P2.0 Privacy Criteria Related to Choice and Consent 27
 - P3.0 Privacy Criteria Related to Collection..... 30
 - P4.0 Privacy Criteria Related to Use, Retention, and Disposal 33
 - P5.0 Privacy Criteria Related to Access 35
 - P6.0 Privacy Criteria Related to Disclosure and Notification..... 37
 - P7.0 Privacy Criteria Related to Quality..... 43
 - P8.0 Privacy Criteria Related to Monitoring and Enforcement 44
 - Common Criteria for the Privacy Category 45
 - Control Environment 45
 - Communication and Information..... 53
 - Risk Assessment 58
 - Monitoring Activities..... 63
 - Control Activities..... 65
 - Logical and Physical Access Controls..... 68
 - System Operations..... 85
 - Change Management 96
 - Risk Mitigation..... 102

**SECTION I:
ASSERTION OF PAYBYPHONE TECHNOLOGIES, INC.
MANAGEMENT**

ASSERTION OF PAYBYPHONE TECHNOLOGIES, INC. MANAGEMENT

We have prepared the accompanying description in section III titled “PayByPhone Technologies, Inc.’s Description of Its Payment Processing Services System Related to Privacy” throughout the period November 1, 2022, to October 31, 2023, (description), based on the criteria for a description of a service organization’s system in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the payment processing services system related to privacy that may be useful when assessing the risks arising from interactions with PayByPhone Technologies, Inc.’s system, particularly information about system controls that PayByPhone Technologies, Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

PayByPhone Technologies, Inc. uses Amazon Web Services (AWS) for cloud infrastructure services, Network Merchants for payment gateway platform services, Accertify for payment gateway platform services, Worldline (fka Ingenico eCommerce Solutions/Ogone) for payment solution services, Valtix for cloud security services, Apigee for full lifecycle API management services, and Twilio for IVR systems services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PayByPhone Technologies, Inc., to achieve PayByPhone Technologies, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents PayByPhone Technologies, Inc.’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of PayByPhone Technologies, Inc.’s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at PayByPhone Technologies, Inc., to achieve PayByPhone Technologies, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents PayByPhone Technologies, Inc.’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of PayByPhone Technologies, Inc.’s controls.

We confirm, to the best of our knowledge and belief, that

- a. the description presents PayByPhone Technologies, Inc.’s payment processing services system related to privacy that was designed and implemented throughout the period November 1, 2022, to October 31, 2023, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that PayByPhone Technologies, Inc.’s service commitments and system requirements would be achieved

based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of PayByPhone Technologies, Inc.'s controls throughout that period.

- c. the controls stated in the description operated effectively throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of PayByPhone Technologies, Inc.'s controls operated effectively throughout that period.

SECTION II: INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Jonny Combe
President and CEO
PayByPhone Technologies, Inc.
600-1290 Homer Street, 6th Floor
Vancouver, BC
V6B 2Y5, Canada

Scope

We have examined PayByPhone Technologies, Inc.'s accompanying description in section III titled "PayByPhone Technologies, Inc.'s Description of Its Payment Processing Services System Related to Privacy" throughout the period November 1, 2022, to October 31, 2023, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

PayByPhone Technologies, Inc. uses Amazon Web Services (AWS) for cloud infrastructure services, Network Merchants for payment gateway platform services, Accertify for payment gateway platform services, Worldline (fka Ingenico eCommerce Solutions/Ogone) for payment solution services, Valtix for cloud security services, Apigee for full lifecycle API management services, and Twilio for IVR systems services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PayByPhone Technologies, Inc., to achieve PayByPhone Technologies, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents PayByPhone Technologies, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of PayByPhone Technologies, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at PayByPhone Technologies, Inc., to achieve PayByPhone Technologies, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents PayByPhone Technologies, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of PayByPhone Technologies, Inc.'s controls. Our examination did not include such

complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

PayByPhone Technologies, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements were achieved. In section I, PayByPhone Technologies, Inc. has provided its assertion titled "Assertion of PayByPhone Technologies, Inc. Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. PayByPhone Technologies, Inc. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section IV, "Trust Services Category, Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

- a. the description presents PayByPhone Technologies, Inc.'s payment processing services system related to privacy that was designed and implemented throughout the period November 1, 2022, to October 31, 2023, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of PayByPhone Technologies, Inc.'s controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that PayByPhone Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls

and complementary user entity controls assumed in the design of PayByPhone Technologies, Inc.'s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of PayByPhone Technologies, Inc., user entities of PayByPhone Technologies, Inc.'s payment processing services system related to privacy during some or all of the period November 1, 2022, to October 31, 2023, business partners of PayByPhone Technologies, Inc. subject to risks arising from interactions with the payment processing services system related to privacy, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

February 2, 2024

**SECTION III:
PAYBYPHONE TECHNOLOGIES, INC.'S DESCRIPTION
OF ITS PAYMENT PROCESSING SERVICES SYSTEM
RELATED TO PRIVACY**

SERVICES PROVIDED

PayByPhone Technologies, Inc. (PayByPhone) functions as both a business-to-business and business-to-business-to-consumer organization. Business-to-business-to-consumer operations allow PayByPhone consumers to pay for on-street or off-street parking with their phone without using a parking meter. The service allows motorists with several different options and features, including the following:

- A SMS reminder before a parking session expires
- Ability to extend parking sessions remotely
- Transaction reporting
- Email parking receipts
- Parking authority notifications

The business-to-business operations allows parking operators to increasingly recognize that mobile payments can both reduce the costs associated with operating expensive pay and display machines as well as increasing revenue per parking session. In addition to lowering operational costs, PayByPhone also provides detailed analytics and professional services for the parking industry.

Client Sales and Onboarding

Internal sales personnel respond to requests for proposal (RFPs) and other sales leads to identify cities, counties, or government entities and individual parking companies that could potentially use PayByPhone services. Once a contract is signed, a project manager, implementation manager, and occasionally a client success member is assigned to the project. Onboarding is tracked through Google Sheets or Microsoft Excel spreadsheets and corresponding checklists. Suppliers are engaged to produce parking signs.

Using an emailed Excel spreadsheet, PayByPhone collects information related to the locations and parking spaces covered in the services, pricing, portal users and permissions, and financial details to facilitate payment collection and disbursements. The implementation manager uses the information to setup an account in the PayByPhone Backoffice application using all the provided details. A portal training session is provided to introduce client personnel to the portal and to demonstrate all of the features for the client's locations. Testing is performed with the client to validate proper configurations. Immediately following the go-live event, clients are transitioned to the Client Success Account Manager team for long-term support.

Clients use the Backoffice application to generate activity-related reports such as space and lot usage and monthly revenues related to the city or business. As needed, ongoing client support is provided the Client Success Account Manager.

Ongoing Transaction Processing and Support

Once live, parking users can use cell phones to connect to the IVR system or cell phone. Users can also use web-based applications to connect to the online system to make payments. Cardholder data (CHD) and personally identifiable data (PII) is transmitted from the cell phone and web-based

application frontends to an application programming interface (API) over Transport Layer Security (TLS) v1.2 for processing and storage. Data can also be received via Twilio's IVR service, which connects to Apigee API platform and forwards PayByPhone-specific traffic. Apigee forwards the data over a mutually authenticated TLS (mTLS) session to an Amazon Web Services (AWS) web application firewall (WAF), where the traffic is decrypted on the Nginx system. The data is then re-encrypted and sent via HTTPS or TLS over virtual private cloud (VPC), where it is decrypted and passed to AWS Lambda functions. AWS Lambda is the interface point between Twilio IVR systems and PayByPhone's IVR systems in the eStructure data center. AWS Lambda makes an API call over TLS 1.2 and routed through AWS Transit Gateway and Valtix Gateway Hub to the load balancer or API, which resides at the eStructure data center.

Additionally, channels are in place in order for consumers to engage PayByPhone for support. The Yoummday (fka ICON) third party provides Zendesk-driven support to consumers. The vendor works incoming Zendesk tickets and resolves issues as they are able. Tier 2 support is escalated to an internal team within PayByPhone, and Tier 3 support is escalated to the Development team using a Jira ticket.

Client Offboarding

Offboarding starts once a client has provided notification that the relationship is to be terminated. A departure date is set, and on that date, the project manager stops the services and merchant accounts in Backoffice. Clients continue to have access to Backoffice to generate reports for 30 days, or longer if agreed on at the termination notification. Once this date has passed, the project manager removes all access for the client in Backoffice.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

The organization adheres to regulatory measures that impact its operations. The Data Protection Policy establishes data governance practices that define the organization's process of managing the availability, usability, integrity, and security of the data in enterprise systems in accordance with all legal, regulatory, compliance, and business requirements. PayByPhone adheres to the following business and regulatory compliance requirements:

- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- Canadian Consumer Privacy Protection Act (CPPA)
- European Union General Data Protection Regulation (GDPR)
- Payment Card Industry Digital Security Standards (PCI DSS)
- California Consumer Privacy Act (CCPA)

Contractual Commitments

Contractual materials are used to communicate descriptions of services to the organization's clients. The descriptions of services and responsibilities are documented in contracts, which must be established before services are provided. The contracts include the following:

- Intellectual property rights
- Definition of and responsibilities pertaining to "client data"
- Definition of and responsibilities pertaining to "Customer" (parker) data
- Mutual indemnification
- Mutual confidentiality and non-disclosure
- Survival of specific clauses in the event of contract termination (specifically, confidentiality, intellectual property, and indemnification clauses)
- PayByPhone responsibility to maintain PCI DSS compliance

System Design

PayByPhone designs its payment processing services system to meet its regulatory and contractual commitments related to privacy. These commitments are based on the services that PayByPhone provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that PayByPhone has established for its services. PayByPhone establishes operational privacy requirements in its system design that support the achievement of its regulatory and contractual commitments. These privacy requirements are communicated in PayByPhone's system policies and procedures, system design documentation, and contracts with clients.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

The privacy category and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Privacy criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services privacy criteria are included in section IV of this report. Although the applicable trust services criteria and related controls are included in section IV, they are an integral part of PayByPhone's description of its payment processing services system related to privacy.

Control Environment Relevant to Privacy

Notice and Communication of Objectives Related to Privacy

PayByPhone has policies and training in place to communicate privacy practices to data subjects and employees. PayByPhone communicates privacy practices and commitments to end users via the Privacy Policy on the company website, which sets out rights of data subjects and PayByPhone's privacy obligations. All employees are informed of their privacy and confidentiality obligations through agreements and training. The Manager of Security & IT Compliance, the Legal Counsel, and the Data Protection Officer (DPO) are responsible for overseeing privacy and compliance activities. All employees and contractors sign a Protection of Corporate Interests Agreement that includes obligations for employees to keep confidential any information related to existing and potential customers of PayByPhone. All employees participate in information security, privacy, and compliance training during onboarding and annually thereafter.

Choice and Consent

Choices regarding the collection, use, retention, disclosure, and disposal of personal information, along with possible consequences of each choice, are communicated to relevant data subjects through the Privacy Policy, GDPR notice, and Terms and Conditions. Customers are given access to the Terms & Conditions, Privacy Policy, and Cookies Policy through the company website and applications.

Customers are required to explicitly accept PayByPhone's terms and conditions to consent to data processing. Customers download the PayByPhone mobile applications from Google Play or the Apple App Store onto their personal devices, and when creating an account, they must accept PayByPhone's terms and conditions. Failure to accept PayByPhone's terms and conditions denies access to PayByPhone application and denies the ability to continue and use the PayByPhone application. Within the mobile application, users must give explicit consent to allowing PayByPhone to send notifications to the user and to allow the application to use the user's location. The data subjects can choose to provide personal information that exceeds the minimum required personal information, such as credentials from third party applications and location information. Data subjects can stop sharing additional personal information and can withdraw consent, and through the Privacy Policy data subjects are made aware of the

consequences for obtaining consent. Additionally, a Cookie Policy is available on PaybyPhone's website and discloses the data subject's ability to choose to disallow certain cookies and the consequences of blocking those cookies on user experience on the website and with the company's services.

Collection

The organization collects personal information in accordance with requirements defined in the Privacy Policy and in compliance with all applicable privacy laws. PayByPhone collects personal data in accordance with the Privacy Policy and is committed to complying with all applicable privacy laws, including without limitation the Canadian PIPEDA and the GDPR. Under the GDPR, personal data refers to information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier. PayByPhone only collects and processes personal data from end users that is required to create a PayByPhone account, to offer services, and to communicate to such users.

End users consent to these conditions with the usage of PayByPhone applications, systems, and services, and the end user is given access to the Terms & Conditions, Privacy Policy, and Cookies Policy. End users agree to the usage and terms when selecting the Agree & Register button. Additionally, through the Privacy Policy, end users are provided with the consequences for denying or withdrawing consent of obtaining or storing personal data.

Use, Retention, and Disposal

The personal data collected from end users is the minimal needed to support the services provided. Personal information is retained in accordance with defined objectives related to privacy and regulations. The Information Security Policies and Procedures have been established and define the timelines for data to be retained; data retention is based on general business requirements and considers PCI DSS requirements due to the nature of business performed.

The organization has a process for destroying and disposing of data and media when no longer needed. In accordance with the Disposal Policy, all electronic and hardcopy data, when no longer needed for legal, regulatory, or business requirements, must be securely deleted from PayByPhone systems. Before computer or communications equipment can be sent to a vendor for trade-in, servicing or disposal, all cardholder data must be destroyed or removed according to the approved methods. Outsourced destruction of media containing cardholder data must use a disposal vendor that provides a Certificate of Destruction. Media that can be re-used must have the data securely deleted and wiped using a utility approved by the Systems Group. PayByPhone has the following requirements in place for destroying media:

- Hard disks are sanitized using a National Institute of Standards and Technology (NIST) 800-88 standard degauss or crosscut shred to, or by penetrating the disk platters with one or more half inch holes drilled through them
- Floppy disks are disintegrated, incinerated, pulverized, crosscut shred, or melted
- Tape media are degaussed, crosscut shred, incinerated, pulverized, or melted
- USB thumb drives, smart cards, and digital media are incinerated, pulverize, or melted
- Optical disks (CDs and DVDs) are destroyed, incinerated, pulverized, crosscut shred, or melted

Access

End users have the right to request access to their personal information and ensure that it remains accurate. The Privacy Policy provides data subjects with a physical mailing address and an email address where they can send their request for access, and defined processes are in place for altering personal information in accordance with information provided by data subjects. End users enter their own information into the PayByPhone applications and system and are responsible for the accuracy of the information entered into the PayByPhone systems. Registered PayByPhone users can use the app or website to access or modify their personal data. Users can also request corrections to PayByPhone directly by emailing the DPO.

Disclosure and Notification

The process for the sharing and disclosure of information with third parties is described in the Terms and Conditions and Privacy Policy, which data subjects consent to upon account creation. PayByPhone only discloses personal data to third parties when there is a lawful basis to do so and does not sell personal data to third parties. PayByPhone does not share personal information with third parties, except as required to offer PayByPhone services or as specifically consented to by users. Users who choose to use the mobile application must also consent to the Terms and Conditions and the Privacy Policy. Contracts between PayByPhone and service providers are established that include restrictions on the use of personal data to only the services referenced in the contract and requirements to provide appropriate safeguards for personal data.

Processes are in place for the creation and retention of a record of authorized and unauthorized disclosures of personal information. The organization has the appropriate technical and organizational protection measures in place to protect personal data from unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks. Requests for authorized disclosures are reviewed by customer service and the DPO and supported by a support ticket. Additionally, PayByPhone has the ability to provide an inventory of personal information that has been collected and stored on data subjects, and the inventory can be provided upon request. Detected or reported unauthorized disclosures of personal information are reviewed by the DPO and the Customer Service team supported by a support ticket.

Processes are in place for the creation and retention of a record of detected or reported unauthorized disclosures of personal information. The Incident Response document and the Security Incident Response Policy require the creation of a Privacy Breach Checklist Report by the DPO or privacy contact person whenever an unauthorized disclosure involves personal data. All breaches of personal data and sensitive information must be documented. PayByPhone also maintains a formally documented Guideline for Analyzing and Reporting a Data Breach to the Authorities and Data Subjects, which is designed to supplement to the Incident Response Policy that serves as a response plan for handling personal data breaches including step by step instructions, the deadlines for completion, and the required activity in the incident ticket for each step. PayByPhone used a specific Slack channel to communicate strategies, roles, and responsibilities, change management tickets are used to document the fix to the issue that caused the security incident, and then lessons learned are documented in a master Security Incident Response ticket.

PayByPhone obtains privacy commitments from vendors and other third parties who have access to personal information to meet defined objectives related to privacy. Vendors and third parties must sign a non-disclosure agreement (NDA) and Data Processing Agreement. The mutual NDA that binds each receiving party to hold confidential information as disclosed by the disclosing party, and the agreement requires that the receiving party protects the information with no less than reasonable care and consistent with the measures it would take to protect its own confidential information. Data Processing Agreements are also established to define the ownership of data and the responsibilities of the obligations of the vendor.

Breach notification procedures address how Data subjects and other relevant individuals are notified of breaches and incidents. The Breach Notification Procedures outline the following steps regarding response and notification:

1. Identification
 - a. Determine if the incident qualifies as a data breach
 - b. If it is a breach and data is processed as a data processor or joint controller, inform the facility
2. Evaluation and risk analysis
 - a. Determine the type of breach and the category of data affected
 - b. Assess the amount of data and the number of data subjects affected
 - c. Create a linked issue in a dedicated ticket
3. Taking appropriate measures
 - a. Identify measures to remedy the breach and mitigate its consequences
 - b. Document them in the main ticket
4. Decision about notifications
 - a. Determine if the breach needs to be reported to the supervisory authority
 - b. Assess if affected data subjects need to be notified
 - c. Document the final decisions and reasoning
5. Notification of group companies
 - a. Inform the responsible contact point
 - b. Document the notification details

The procedures also include two breach notification templates, including the content required to disclose the breach to data subjects: one template is for EU end users and one template is for California end users. The DPO or relevant privacy employee is responsible for notifying external parties about personal data breaches. The Incident Response document and the Security Incident Response Policy includes breach notification requirements for various jurisdictions, Canada, European countries, and certain US states as well as links to breach notification reporting forms for those jurisdictions.

Quality

The organization ensures that all information within the systems and applications is kept up to date, accurate, complete, and relevant. Users may request a correction of personal data to ensure its accuracy and completeness. The request to correct personal data must be made in writing and provide sufficient detail to identify the personal data and the correction being sought. If such personal data is demonstrated to be inaccurate or incomplete, PayByPhone will, so far as practicable, and as soon as practicable, correct such the personal data as required and sends the

corrected information to any organization that PayByPhone disclosed the personal data to in the previous year. If a correction is not made, PayByPhone notes the correction request in that individual's file.

Monitoring and Enforcement

The organization has a process for managing the receipt, addressing, resolution, and communication of inquiries, complaints, and disputes related to the organization privacy practices.

Risk Assessment Process

PayByPhone conducts risk assessments annually and following significant changes to the environment to identify new threats and vulnerabilities, and the NIST 800-30 methodology is followed when conducting the risk assessment. The Systems Group and the IT Operations (ITOPS) team is responsible for conducting the risk assessment, informing the company about information security issues and vulnerabilities, assigning risk ranks to the new risks and vulnerabilities, and identifying and implementing the appropriate controls to mitigate any new risks. The Jira enterprise risk management (ERM) tool is used to track both enterprise risks and IT risks, which are also captured in the risk register. Each risk is tracked separately and includes a description of the risk, risk category, likelihood, impact, risk type, and risk owner. New risks are provided to the Compliance or IT Security team through leaders of other teams. The Compliance team and IT Security team meet monthly to discuss new risks and review old ones in the Jira ERM register.

Rate limiting and geo-IP controls have been implemented through Apigee as a method to limit the risk of SMS and parking renewal bot fraud executed by external attackers against the system. Terraform and AWS Guardrails prevent misusing AWS account resources for unintended purposes, and Backoffice databases capture all events involving creating, reading, updating, and deleting application records through Backoffice, which mitigates the risk of fraud through changing the Merchant of Record information for client parking transactions.

Information and Communication Systems

The Systems Groups maintain the formally documented Information Security Policies and Procedures that define general control activities over technology. The Information Security Policies and Procedures is a single, comprehensive information security policy covering a range of topics, each in their own top-level section; the topics include the following:

- Roles and responsibilities for managing the information security program
- Change management
- Data classification and control
- Background checks
- Data retention and disposal
- Paper and electronic media
- Firewall, router, and switch security administration
- Configuration management
- Antivirus
- Backups
- Encryption of data at rest and in transit
- Software development and lifecycle management
- Incident response
- Employee identification
- Logging controls
- Service providers and third parties

- Detecting failures of critical security controls
- Internal audit of security controls
- Security awareness
- System configuration standards

The organization maintains a formally documented Security Awareness and Acceptable Use Policy that includes provisions for end-user use of PayByPhone assets. The policy defines prohibited actions pertaining to PayByPhone data and systems, and it defines critical technologies to include internet, intranet, and extranet-related systems, including computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and File Transfer Protocol (FTP).

The policies and procedures define the information security responsibilities for personnel. The Systems Groups, including Cloud Platforms and Corporate IT, are responsible for detailed policies and procedures as well as implementation of controls on PayByPhone’s information systems, reviewing relevant information security logs, and administering user accounts, among other responsibilities. Users are responsible for understanding the consequences of their actions, maintaining awareness of policies, attending security awareness training, and remaining knowledgeable of data classification and handling requirements.

Monitoring Controls

PayByPhone has monitoring activities in place to ensure operational quality and control. Operational quality and control are managed through site reliability management (SRM) principles, which create a framework for the observability of IT systems and the related incident or service management processes and metrics to monitor the service. The SRM is responsible for establishing reliability expectations for all other engineering teams to follow, including internal service-level agreements (SLAs) (99.9%). In some cases, SLAs can also be committed to external customers. Jira tickets are used to track operational errors experienced in the production environment, and Datadog is used to monitor various services within the production application and to notify operations staff via PagerDuty. Datadog provides metrics and dashboards accessible to both business and technical staff. The metrics monitored include transaction and order processing metrics with a focus on credit card processing metrics tracking the number of transactions, including both successful and unsuccessful, and platform reliability (site reliability) metrics that track platform availability across the PayByPhone technology components.

Real-time monitoring of payment transactions is in place, with alerts triggered for a specified number of failures or declines over a specific timeframe. Alerts are sent via PagerDuty to the on-call PayByPhone support personnel, who assess and address the issue, often by disabling suspicious motorist accounts. Project monitoring is facilitated through Confluence, and regular project updates are provided to the Executive team. PayByPhone uses the Payment Processor Runbook to diagnose and remediate various processing errors that can occur on the platform.

Changes to the System Related to Privacy During the Period

The following changes, which are likely to affect report users’ understanding of the payment processing services system, occurred during the period from November 1, 2022, through October 31, 2023.

Description of Change	Effect of the Change on the System	Date of Change
PayByPhone migrated data center-applications and infrastructure to AWS.	<p>Auditor learned through interviews that PayByPhone recently transitioned all applications out of a contracted colocation facility and into AWS. This transitioned resulted in numerous operational changes as PayByPhone transitioned from the legacy, virtual machine-based delivery model to one that is based almost entirely on modern DevOps principles using cloud-provided infrastructure.</p> <p>During the decommissioning process, PayByPhone commissioned Dataknox.io to destroy all media from data center-located systems.</p>	Ongoing throughout the audit period, with final completion May 2023
PayByPhone was sold by Volkswagen Financial Services (VWFS) to FLEETCOR.	There were no meaningful changes within this audit period as a direct result of the sale; however, future changes could be expected in the implementation of controls currently performed by VMFS.	September 2023

COMPLEMENTARY USER-ENTITY CONTROLS

PayByPhone's services are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. PayByPhone's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. PayByPhone also provides best practice guidance to clients regarding control element outside the sphere of PayByPhone responsibility.

This section describes additional controls that should be in operation at user organizations to complement the PayByPhone controls. Client Consideration recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with PayByPhone.
- User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with PayByPhone's services.
- Transactions for user organizations relating to PayByPhone's services should be appropriately authorized, and transactions should be secure, timely, and complete.
- For user organizations sending data to PayByPhone, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
- User organizations should implement controls requiring additional approval procedures for critical transactions relating to PayByPhone's services.
- User organizations should report to PayByPhone in a timely manner any material changes to their overall control environment that may adversely affect services being performed by PayByPhone.
- User organizations are responsible for notifying PayByPhone in a timely manner of any changes to personnel directly involved with services performed by PayByPhone. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by PayByPhone.
- User organizations are responsible for adhering to the terms and conditions stated within their contracts with PayByPhone.
- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by PayByPhone.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION IV: TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

APPLICABLE TRUST SERVICES CRITERIA RELEVANT TO PRIVACY

Although the applicable trust services criteria and related controls are presented in section IV, “Trust Services Category, Criteria, Related Controls, and Tests of Controls,” they are an integral part of PayByPhone’s system description throughout the period November 1, 2022, to October 31, 2023.

Privacy

The trust services criteria relevant to privacy address the need for personal information to be collected, used, retained, disclosed, and disposed of to achieve the service organization’s service commitments and system requirements.

Although the confidentiality objective applies to various types of sensitive information, privacy applies only to personal information. The privacy criteria are organized as follows:

- i. *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.
- ii. *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.
- iii. *Collection.* The entity collects personal information to meet its objectives related to privacy.
- iv. *Use, retention, and disposal.* The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.
- v. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.
- vi. *Disclosure and notification.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.
- vii. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.
- viii. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

Common Criteria Related to Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to

systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of

- i. information during its collection or creation, use processing, transmission, and storage and
- ii. systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of PayByPhone's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Trust Services Criteria for the Privacy Category

P1.0 Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.		
P1.1.1	Privacy practices and commitments are communicated to data subjects via the Privacy Policy on the corporate website.	<p>Reviewed the Privacy Policy published on the organization's public website and verified that the Privacy Policy addresses the following:</p> <ul style="list-style-type: none"> • Special notice regarding children under the age of 16 years of age • Who is the data processor • What information is collected and processed • Why information collected is processed (contractual relationship, consent, and legitimate interest) • How the information collected is processed • Who the information collected is shared with • Where information collected is transferred • How information collected is kept safe • Retention of information collection • Data subjects rights regarding information collected • Definitions • Links to app store and other websites • Applicable laws • Changes to the Privacy Policy • Questions and inquiries regarding information collected • How to contact PayByPhone <p>Interviewed the Manager of Security and IT Compliance and determined that PayByPhone communicates privacy practices and commitments to end users via the Privacy Policy on the company website, which sets out rights</p>	No Relevant Exceptions Noted

		of data subjects and PayByPhone’s privacy obligations	
P1.1.2	All employees are informed of their privacy and confidentiality obligations through agreements and training.	<p>Interviewed the Manager of Security and IT Compliance and determined that all PayByPhone employees and contractors sign a Protection of Corporate Interests Agreement that includes obligations for employees to keep confidential any information related to existing and potential customers of PayByPhone</p> <p>Observed the execution of privacy and compliance responsibilities and verified that these responsibilities fall to the Manager of Security & IT Compliance, the Legal Counsel, and the Data Protection Officer (DPO)</p> <p>Observed training materials and verified that the organization provides all employees with information security, privacy, and compliance training during the employee onboarding process and annually thereafter; all PayByPhone employee’s sign and acknowledge the Protection of Corporate Interest Agreement that address the protection of the organization’s confidential and protected sensitive information</p>	No Relevant Exceptions Noted

Trust Services Criteria for the Privacy Category

P2.0 Privacy Criteria Related to Choice and Consent

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
P2.1	<p>The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.</p>		
P2.1.1	<p>Choices regarding the collection, use, retention, disclosure, and disposal of personal information are communicated to relevant data subjects through the Privacy Policy, GDPR notice, and terms and conditions.</p>	<p>Reviewed the Privacy Policy published on the organization's public website and verified it addresses the following:</p> <ul style="list-style-type: none"> • The data subjects choose to provide personal information that exceeds the minimum required personal information, such as credentials from third party applications and location information • The data subject's ability to stop sharing additional personal information • Data subject's choices about communication from the organization • Data subjects right to withdraw consent • Consequences of withdrawal of consent • Lodging a compliant or inquiry <p>Observed the Cookie Notice on PaybyPhone's website and established that the notice discloses the data subject's ability to choose to disallow certain cookies and the consequences of blocking those cookies on user experience on the website and with the company's services</p> <p>Observed the Privacy Preference Center on PaybyPhone's website and confirmed the data subject's ability to manage cookie consent preferences</p>	<p>No Relevant Exceptions Noted</p>

		<p>Observed the General Data Protection Regulation (GDPR) and PayByPhone article on the company website and verified that the GDPR notice contains the following key elements:</p> <ul style="list-style-type: none"> • Consent per GDPR • Data subjects rights under GDPR • Links to additional privacy information (Terms and Conditions, Privacy Policy, and Cookies Policy) • Contact information <p>Observed PayByPhone Terms & Conditions document and verified it addresses the following key areas:</p> <ul style="list-style-type: none"> • Account creation and consent • Responsibility for information accuracy • Account use and responsibilities • Service-level guarantees • Dispute resolution and confidential arbitration • Disclosure of account information to third parties • Inquiries • Privacy Policy, Legal Notice, and Cookies Policy • Cancellation of account • Applicable laws • Contact information 	
P2.1.2	<p>Customers are required to explicitly accept PayByPhone’s terms and conditions to consent to data processing.</p>	<p>Reviewed the Privacy Policy published on the organization’s public website and verified it addresses requirements for obtaining consent and the consequences for data subjects and PayByPhone when consent is withdrawn</p> <p>Observed that the PayByPhone mobile applications are available from Google Play and Apple App Store, where they are downloaded, and from there a user account is created and verified that, during the account creation process, users must accept PayByPhone’s terms and conditions; failure to accept PayByPhone’s terms and conditions denies access to PayByPhone</p>	<p>No Relevant Exceptions Noted</p>

		<p>application and denies the ability to continue and use the PayByPhone application</p> <p>Observed phone application and web-based application registration processes and verified that the end user is given access to the Terms & Conditions, Privacy Policy, and Cookies Policy and agree to the usage and terms when selecting Agree & Register.</p> <p>Observed user notifications and privacy settings in the mobile application and verified that separate explicit consent is required via a toggle for PayByPhone to process personal data for each of the following purposes:</p> <ul style="list-style-type: none"> • Feedback and surveys • New features • Promotions and discounts • Partner marketing • Personalized offers • Online advertising through third parties 	
--	--	--	--

Trust Services Criteria for the Privacy Category

P3.0 Privacy Criteria Related to Collection

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.		
P3.1.1	<p>The organization collects personal information in accordance with requirements defined in the Privacy Policy and in compliance with all applicable privacy laws.</p>	<p>Reviewed the Privacy Policy and verified that it addresses components of the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and European Union GDPR</p> <p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> • Personal data refers to information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier • PayByPhone collects personal data in accordance with the Privacy Policy and is committed to complying with all applicable privacy laws, including without limitation the Canadian PIPEDA and the GDPR • PayByPhone only collects and processes personal data from end users that is required to create a PayByPhone account, to offer services, and to communicate to such users <p>Observed an example of the PayByPhone Mobile Application Personal Information Assessment and verified that the assessment addresses the following areas:</p> <ul style="list-style-type: none"> • Data inventory of the data elements collected • Use of the data collected • Reason for data collection 	<p>No Relevant Exceptions Noted</p>

		<ul style="list-style-type: none"> • Consent for data collection • Protection of data collected 	
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity’s objectives related to privacy.		
P3.2.1	Consent for collection and use of personal data is obtained when the data subject registers for company services, systems, and applications.	<p>Reviewed the Privacy Policy published on the organization’s public website and verified it addresses the requirement for granting consent as well as the consequences for withdrawing consent</p> <p>Observed PayByPhone Terms & Conditions document and verified it addresses the following key areas:</p> <ul style="list-style-type: none"> • Account creation and consent • Responsibility for information accuracy • Account use and responsibilities • Service-level guarantees • Dispute resolution and confidential arbitration • Disclosure of account information to third parties • Inquiries • Privacy Policy, Legal Notice, and Cookies Policy • Cancellation of account • Applicable laws • Contact Information <p>Observed that the PayByPhone mobile applications are available from Google Play and Apple App Store, where they are downloaded, and from there a user account is created and verified that, during the account creation process, users must accept PayByPhone’s terms and conditions; failure to accept PayByPhone’s terms and conditions denies access to PayByPhone application and denies the ability to continue and use the PayByPhone application</p> <p>Observed PayByPhone mobile application requests consent to send</p>	No Relevant Exceptions Noted

		notifications to the user and to allow the application to use the user's location and verified that the user must give explicit consent in both cases	
--	--	---	--

Trust Services Criteria for the Privacy Category

P4.0 Privacy Criteria Related to Use, Retention, and Disposal

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.		
P4.1.1	The personal data collected from end users is the minimal needed to support the services provided.	<p>Interviewed the Manager of Security and IT Compliance and determined that the Privacy Policy defines the use of personal information in accordance with applicable data protection laws</p> <p>Observed an example of the PayByPhone Mobile Application Personal Information Assessment and verified that the assessment addresses the following areas:</p> <ul style="list-style-type: none"> • Data inventory of the data elements collected • Use of the data collected • Reason for data collection • Consent for data collection • Protection of data collected <p>Observed the PayByPhone app and the account creation process and verified that the personal information collected is minimal</p>	No Relevant Exceptions Noted
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.		
P4.2.1	Personal information is retained in accordance with defined objectives related to privacy and regulations.	<p>Reviewed the Information Security Policies and Procedures (dated July 11, 2023) and verified that the following data handling requirements are defined:</p> <ul style="list-style-type: none"> • Data retention • Data disposal • CHD retention and purging <ul style="list-style-type: none"> ○ Stale CHD data is purged after 36 months ○ Expired CHD will be purged after nine months <p>Interviewed the Manager of Security and IT Compliance and determined that when the PEER1 data center systems were decommissioned as part</p>	No Relevant Exceptions Noted

		<p>of the transition to a cloud-only application delivery model, the assets in the data center were physically destroyed by a third party</p> <p>Observed records for three recently deactivated customers (parking authorities) and verified evidence of decommissioning customer accounts</p>	
P4.3	The entity securely disposes of personal information to meet the entity’s objectives related to privacy.		
P4.3.1	<p>The organization securely disposes of personal information to meet objectives related to privacy.</p>	<p>Reviewed the Disposal Policy and verified that the following are enforced:</p> <ul style="list-style-type: none"> • All cardholder electronic or hardcopy data, when no longer needed for legal, regulatory, or business requirements, must be securely deleted from PayByPhone systems using company-approved method • A programmatic (automatic) process is executed when a customer enters a new credit card; the old credit card is removed and the new card inserted • Other applicable data stored in files and directories where the containing media is re-used must be deleted securely by a wiping utility approved by the Systems Group <p>Observed a completed Certificate of Destruction from DataKnox.io and verified that data was destroyed in accordance with NIST 800-53</p> <p>Observed a completed Certificate of Destruction from Infoshred and verified that third parties are used to destroy data</p>	<p>No Relevant Exceptions Noted</p>

Trust Services Criteria for the Privacy Category

P5.0 Privacy Criteria Related to Access

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.		
P5.1.1	End users have the right to request access to their personal information.	<p>Reviewed the Privacy Policy available on the company website and verified that data subjects are provided with a physical mailing address and an email address in order to request access to the personal data collected</p> <p>Interviewed the Manager of Security and IT Compliance and determined that users can request a copy of their personal data by submitting a data access request as described in the Privacy Policy under section Access</p> <p>Observed a Zendesk ticket that includes a subject access request and the accompanying email chain and verified that data subjects can request access to collected data</p>	No Relevant Exceptions Noted
P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.		
P5.2.1	Defined processes are in place for altering personal information in accordance with information provided by data subjects.	<p>Interviewed the Manager of Security and IT Compliance and determined that registered PayByPhone users can use the app or website to access or modify their personal data that they provide to PayByPhone and is associated with their account to ensure its accuracy; users can also request corrections to PayByPhone directly but no correction requests were submitted during the audit period</p> <p>Observed the use of mobile applications and verified that users can update and modify their personal</p>	No Relevant Exceptions Noted

		<p>information directly within the application</p> <p>Observed the emails sent to dpo@PayByPhone.com and verified that data subject requests can be submitted to PayByPhone as instructed in the Privacy Policy, and that none of the data subject requests submitted within the audit period were data amendment requests</p>	
--	--	--	--

Trust Services Criteria for the Privacy Category

P6.0 Privacy Criteria Related to Disclosure and Notification

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.		
P6.1.1	The process for the sharing and disclosure of information with third parties is described in the Privacy Policy, which data subjects consent to upon account creation.	<p>Reviewed the Privacy Policy on the company website and verified that the policy discloses:</p> <ul style="list-style-type: none"> • PayByPhone only discloses personal data to third parties when there is a lawful basis to do so • PayByPhone does not sell personal data to third parties • Examples of third-party disclosures related to the application services, such as confirming parking sessions, web hosting, event logging, customer service, payment processing, government agencies, and law enforcement <p>Interviewed the Manager of Security and IT Compliance and determined that PayByPhone does not share personal information with third parties, except as required to offer PayByPhone services or as specifically consented to by users</p> <p>Observed user account creation in the application and verified that users who choose to use the mobile application must also consent to the Terms and Conditions and the Privacy Policy</p> <p>Observed a list of PayByPhone PCI third party service providers and verified that the documentation includes the purpose for disclosing data to each third party, and that the third parties perform the services listed in the Terms and Conditions and Privacy Policy</p> <p>Observed contracts between PayByPhone and service providers and</p>	No Relevant Exceptions Noted

		verified that it that includes restrictions on the use of personal data to only the services referenced in the contract and requirements to provide appropriate safeguards for personal data	
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity’s objectives related to privacy.		
P6.2.1	Processes are in place for the creation and retention of a record of authorized disclosures of personal information.	<p>Reviewed the Privacy Policy and verified that the policy includes language on how PayByPhone never uses or discloses personal data unless there is a lawful basis to do so; requests for authorized disclosures are reviewed by customer service and the DPO and are supported by a support ticket</p> <p>Interviewed the Manager of Security and IT Compliance and determined that PayByPhone has processes for the creation and retention of a record of authorized disclosures of personal information as described in the Privacy Policy</p>	No Relevant Exceptions Noted
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity’s objectives related to privacy.		
P6.3.1	Processes are in place for the creation and retention of a record of detected or reported unauthorized disclosures of personal information.	<p>Reviewed the Incident Response document and the Security Incident Response Policy and verified that they address the process for incidents and data breaches, including the unauthorized disclosure of personal information; specifically, the policy requires the creation of a Privacy Breach Checklist Report by the DPO or privacy contact person whenever an unauthorized disclosure involves personal data; and all breaches of personal data and sensitive information must be documented as required in the policy</p> <p>Reviewed Guideline for Analyzing and Reporting a Data Breach to the Authorities and Data Subjects and verified that it is designed to supplement to the Incident Response</p>	No Relevant Exceptions Noted

		<p>Policy that serves as a response plan for handling personal data breaches including step by step instructions, the deadlines for completion, and the required activity in the incident ticket for each step</p> <p>Interviewed the Manager of Security and IT Compliance and determined that PayByPhone has processes for the creation and retention of a record of unauthorized disclosures of personal information as described in the Privacy Policy; the organization has the appropriate technical and organizational protection measures in place to protect personal data from unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks; and detected or reported unauthorized disclosures of personal information are reviewed by the Data Protection Officer and the Customer Service team supported by a support ticket</p> <p>Observed a sample incident response documentation (there were no incidents that involved personal data) and verified that PayByPhone uses a specific Slack channel to communicate strategies, roles, and responsibilities, change management tickets are used to document the fix to the issue that caused the security incident, and then lessons learned are documented in a master Security Incident Response ticket</p>	
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity’s objectives related to privacy. The entity assesses those parties’ compliance on a periodic and as-needed basis and takes corrective action, if necessary.		
P6.4.1	The organization obtains privacy commitments from vendors and other third parties who have access to personal information to meet defined objectives related to privacy.	Reviewed the Information Security Policies and Procedures and verified that requirements for PayByPhone to maintain a written agreement with service providers that requires the service provider to acknowledge their responsibility for the security of the	No Relevant Exceptions Noted

		<p>data they process on behalf of PayByPhone</p> <p>Interviewed the Manager of Security and IT Compliance and determined that the process for sharing and disclosure of information with third parties is described in the Privacy Policy; PayByPhone requires vendors to sign non-disclosure agreements and contracts to meet company requirements; and PayByPhone involves its legal team to review the contracts</p> <p>Observed an example of the Zendesk Data Processing Agreement and verified that the document defines the data processing agreement between Zendesk and PayByPhone, which defines the ownership of data and the responsibilities of the obligations of the vendor</p>	
P6.5	<p>The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity’s objectives related to privacy.</p>		
P6.5.1	<p>The organization uses NDAs to obtain commitments from vendors and other third parties with access to personal information to protect personal information from unauthorized disclosures.</p>	<p>Interviewed the Manager of Security and IT Compliance and determined that PayByPhone signs NDAs with vendors prior to sharing any confidential information</p> <p>Observed the PayByPhone NDA template and verified that it is a mutual NDA that binds each receiving party to hold confidential information as disclosed by the disclosing party, and the agreement requires that the receiving party protects the information with no less than “reasonable care” and consistent with the measures it would take to protect its own confidential information</p> <p>Observed completed contracts and verified that contracts are established between PayByPhone and their</p>	<p>No Relevant Exceptions Noted</p>

		subservice organizations, where the subservice organizations commit to notifying PayByPhone in the event of a security incident	
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity’s objectives related to privacy.		
P6.6.1	Data subjects and other relevant individuals are notified of breaches and incidents in accordance with incident response policies and procedures.	<p>Reviewed the Breach Notification Procedures (dated May 19, 2021) and verified that it addresses the following phases:</p> <ul style="list-style-type: none"> • Identification <ul style="list-style-type: none"> ○ Determine if the incident qualifies as a data breach ○ If it is a breach and data is processed as a data processor or joint controller, inform the facility • Evaluation and risk analysis <ul style="list-style-type: none"> ○ Determine the type of breach and the category of data affected ○ Assess the amount of data and the number of data subjects affected ○ Create a linked issue in a dedicated ticket • Taking appropriate measures <ul style="list-style-type: none"> ○ Identify measures to remedy the breach and mitigate its consequences ○ Document them in the main ticket • Decision about notifications <ul style="list-style-type: none"> ○ Determine if the breach needs to be reported to the supervisory authority ○ Assess if affected data subjects need to be notified ○ Document the final decisions and reasoning • Notification of group companies <ul style="list-style-type: none"> ○ Inform the responsible contact point ○ Document the notification details • The procedures also include two breach notification templates, including the content required to disclose the breach to data 	No Relevant Exceptions Noted

		<p>subjects: one template is for EU end users and one template is for California end users</p> <p>Reviewed the Incident Response document and the Security Incident Response Policy and verified the following:</p> <ul style="list-style-type: none"> • The DPO or relevant privacy employee is responsible for notifying external parties about personal data breaches • The policy includes breach notification requirements for various jurisdictions, Canada, European countries, and certain US states as well as links to breach notification reporting forms for those jurisdictions • The policy creates a preference for directly notifying data subjects about the breach in writing 	
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.		
P6.7.1	The organization has a process for providing data subjects with an inventory of personal information.	<p>Interviewed the Manager of Security and IT Compliance and determined that the organization has the ability to provide an inventory of personal information that has been collected and stored on data subjects, and the inventory can be provided upon request</p> <p>Observed a Zendesk ticket that includes a subject access request and the accompanying email chain and verified that data subjects can request access to collected data</p>	No Relevant Exceptions Noted

Trust Services Criteria for the Privacy Category

P7.0 Privacy Criteria Related to Quality

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.		
P7.1.1	The organization ensures that all information within the systems and applications is kept up to date, accurate, complete, and relevant.	<p>Reviewed the Privacy Policy available on the company website and verified that users may request a correction of personal data in order to ensure its accuracy and completeness</p> <p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> • The request to correct personal data must be made in writing and provide sufficient detail to identify the personal data and the correction being sought • If such personal data is demonstrated to be inaccurate or incomplete, PayByPhone will, so far as practicable, and as soon as practicable, correct such the personal data as required and send the corrected information to any organization that PayByPhone disclosed the personal data to in the previous year • If a correction is not made, PayByPhone will note the correction request in that individual's file 	No Relevant Exceptions Noted

Trust Services Criteria for the Privacy Category

P8.0 Privacy Criteria Related to Monitoring and Enforcement

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.		
P8.1.1	The organization has a process for managing the receipt, addressing, resolution, and communication of inquiries, complaints, and disputes related to the organization privacy practices.	<p>Reviewed the Privacy Policy and verified that it addresses the disclosure of data subject's right to submit a complaint, the respective DPO is responsible for handling complaints, and instructions for submitting a complaint to the DPO via an email address linked in the Privacy Policy</p> <p>Interviewed the Manager of Security and IT Compliance and determined that the organization has a process for the handling data subject requests submitted via the email address provided on the organization's online Privacy Policy</p> <p>Observed inbox for the dpo@PayByPhone.com and verified that the email address received a test email and that there were no privacy complaints submitted to the email address during the audit period</p>	No Relevant Exceptions Noted

Common Criteria for the Privacy Category			
Control Environment			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	The organization relies on leadership and conducts training to ensure that security and compliance are prioritized.	<p>Interviewed the Manager of Security and IT Compliance and determined that the primary directive from management is to ensure compliance; the primary method to achieve this is through education; the compliance program is enforced through a quarterly presentation between the Compliance team and leadership to cover the top five initiatives; and the organization communicates every compliance effort to the PayByPhone Product Steering Board (PSB) to ensure that the compliance program contributes to corporate value</p> <p>Observed Weekly Cyber Posts, townhall meetings notes, and IT security blogs and verified that continuous training is provided to develop a security and compliance-conscious culture</p>	No Relevant Exceptions Noted
CC1.1.2	Corporate policies and company handbooks are used to communicate guidelines and company expectations.	<p>Reviewed the Global Guidelines document and verified that it addresses the following policies:</p> <ul style="list-style-type: none"> • Crisis Communication Guidelines • Guideline for analyzing and reporting a data breach to the authorities and data subjects • Data Subject Request Guideline • PayByPhone Compliance Requirements Overview <p>Reviewed the Global Policies document and verified that it shows top-level principles on specific subject matters, and the following policies are addressed:</p> <ul style="list-style-type: none"> • Data Protection Policy • Data Retention Policy • Global Information Security Policies • Security Incident Response Policy • Background Check Policy 	No Relevant Exceptions Noted

		<p>Reviewed the North American Organizational Handbook and verified that it addresses the following North American policies and guidelines:</p> <ul style="list-style-type: none"> • Remote Work Health & Safety Policy • Sick & Personal Time Off Policy • Time Off Vacation Policy • Equal Employment Opportunity Policy <p>Interviewed the People Business & Operations Partner and determined that the Employee Handbook is maintained in Confluence</p> <p>Observed records for a sample of new hires (4 of 44) and verified that handbooks are acknowledged by new employees</p>	
CC1.1.3	<p>A Code of Conduct is maintained that communicates company values as well as ethical and behavioral expectations to employees.</p>	<p>Reviewed the VWFS Code of Conduct and verified that it includes:</p> <ul style="list-style-type: none"> • Messages regarding integrity and compliance • Social responsibility • Responsibilities to business partners • Commitments to other teammates • Occupational safety and healthcare • Data protection • Security and protection of information • Know-how and intellectual property • IT security • Handling company assets <p>Interviewed the Manager of Security and IT Compliance and determined that the core values of the company are:</p> <ul style="list-style-type: none"> • See through customers' eyes • Work together • Stay curious • Have fun • Make things happen 	<p>No Relevant Exceptions Noted</p>

		Observed records for a sample of new hires (4 of 44) and verified that the onboarding checklist items, including acknowledgement of all company policies and Code of Conduct	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	A management board (M-Board) is established to provide oversight and direction to the organization.	<p>Interviewed the Manager of Security and IT Compliance and determined that the management consists of the Chief Executive Officer (CEO), Chief Financial Officer (CFO), and Chief Technology Officer (CTO)</p> <p>Interviewed the Chief information Security Officer (CISO) & Senior Director of Reliability and determined that the PayByPhone management board (M-Board) consists of the PayByPhone CEO, CTO, and CFO</p> <p>Observed three monthly M-Board agendas and verified that compliance and information security topics are covered, and that the M-Board monthly meeting is established on a regular cadence</p>	No Relevant Exceptions Noted
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	Organization charts are maintained that illustrate the separation of duties, company structure, and reporting lines.	<p>Interviewed the Manager of Security and IT Compliance and determined that Security and IT Compliance reports through the CTO organization as one of three permanent PayByPhone board members (CEO, CTO, and CFO); a process is in place to ensure that certain activities, such as decisions and transaction choices, must be approved by at least two people, and this controlling mechanism is used to facilitate delegation of authority and increase transparency</p> <p>Observed the organization chart and verified that it illustrates the reporting lines, company structure, and separation of duties, and that the</p>	No Relevant Exceptions Noted

		<p>company senior leadership consists of the CEO, CFO and CTO, who are responsible for all day-to-day operations of the company</p> <p>Observed the company’s organization charts in BambooHR and verified that the senior leadership consists of the CEO, CTO, and CFO</p>	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	The organization maintains formally documented job descriptions for personnel.	Observed numerous job descriptions for information security personnel, including CISO & Manager of Compliance and IT Security, Software Engineers, and Security Analysts, and verified that information security concerns were appropriate to each role	No Relevant Exceptions Noted
CC1.4.2	Onboarding activities are outlined in the Employee Onboarding Checklist and are managed in BambooHR to ensure all employees are consistently onboarded.	<p>Interviewed the People Business & Operations Partner and determined that onboarding is managed on the Employee Onboarding Checklist on BambooHR and includes tax forms, eligibility forms, payroll forms, bank deposits, the Protection of Corporate Interests Agreement, and technology onboarding; all employees sign a confidentiality agreement as part of their employment agreement</p> <p>Observed the onboarding task list and verified that the manager’s role in the onboarding process includes preparing an onboarding plan, forwarding recurring calendar invites and inviting the new team member to appropriate Slack channels, and communicating the laptop requirements to the talent acquisition partner; the employee’s tasks in the onboarding process involve reviewing the health and safety information, reviewing the organizational handbook and code of conduct, reviewing the day one orientation files and bookmarking links, and reviewing and signing the company policies</p>	No Relevant Exceptions Noted

		<p>Observed records for a sample of new hires (4 of 44) and verified that the following items are completed:</p> <ul style="list-style-type: none"> • BambooHR Onboarding Checklist • Access request tickets in Jira • Background checks results • Completion of security awareness training • Information security policy acknowledgements <p>Observed the Confidentiality Agreement and verified that they address the terms and conditions of employment with PayByPhone; the agreement mentions issues related to confidentiality, non-competition, non-solicitation, and ownership of work product</p>	
CC1.4.3	All potential employees undergo a background check before being hired.	<p>Reviewed the Information Security Policies and Procedures (dated September 4, 2023) and verified the following:</p> <ul style="list-style-type: none"> • The background check policy applies to all employees and contractors with access to cardholder data • PayByPhone aims to perform background checks for all employees, but there may be exceptions for new residents • Checks should include verification of name, address, and date of birth • Official identification and Social Security number verification is required • Employment and educational verification should be conducted • Credit checks, federal or state criminal record checks, and reference checks are necessary • Drug screenings may be applicable and allowed by law • Protections for PII and background check results are in place 	No Relevant Exceptions Noted

		<p>Interviewed the People Business & Operations Partner and determined that background checks are performed by Sterling in accordance with all local laws and regulations</p> <p>Observed new hire records for a sample of new employees (4 of 44) and verified that the background checks were completed by Sterling</p>	
CC1.4.4	<p>Training and continuous education opportunities are provided to employees via the Inspired eLearning learning management system (LMS).</p>	<p>Reviewed the Security & IT Compliance Onboarding document and verified all new employees must attend and acknowledge completion of the organization’s Security Program, which addresses the following:</p> <ul style="list-style-type: none"> • Awareness training • Risk assessment • Policies and procedures • Business case studies • What is a Security Incident? • Examples of non-public private information (NPPI) • Indications of an attack (security event) • Examples of confidentiality, integrity, and availability incidents • How to respond to when a security incident is detected <p>Interviewed the Manager of Security and IT Compliance and determined that general security awareness training is provided through the Inspired eLearning LMS, and new campaigns are run quarterly to keep training fresh and short for all users; all new hires are provided security awareness training on a bi-monthly schedule where the session is conducted as a live-session (in-person or through web conference, as appropriate)</p> <p>Observed that Security and Compliance team members hold various certifications and verified that</p>	<p>No Relevant Exceptions Noted</p>

		<p>some of the certifications include the following:</p> <ul style="list-style-type: none"> • GIAC Security Essentials (SANS Technology Institute) • GIAC Certified Incident Handler (SANS Technology Institute) • GIAC Public Cloud Security (SANS Technology Institute) • EXIN Information Security ISO 27001 Certificate • CompTIA Cloud Essentials+ certificate • ITIL & RSA Incident Handling <p>Observed the use of Inspired eLearning and verified that it is used to provide security awareness content to all employees, and that the LMS also captures each user’s acknowledgement of their receipt and understanding of the information security policy</p>	
CC1.4.5	<p>The organization has a process in place that outlines how to complete voluntary and involuntary terminations.</p>	<p>Interviewed the People Business & Operations Partner and determined the following:</p> <ul style="list-style-type: none"> • In the event of voluntary termination, the employees must provide a 30-day notice, as stipulated in the Employment Agreement, but the organization attempts to accommodate shorter if needed • The termination process begins in BambooHR and requires submitting a “Joiners and Leavers” ticket in Jira to manage the process with all parties • In the event of involuntary termination, a similar process is followed, but with greater urgency in coordination between all the parties • In both cases, equipment is returned through a courier service and compared against IT asset inventory • The termination process is managed in BambooHR and Jira tickets 	<p>No Relevant Exceptions Noted</p>

		Observed offboarding records for a sample of terminated employees (9 of 93) and verified that the employees were removed from all relevant systems, including BambooHR, Azure Active Directory, and Backoffice	
CC1.4.6	Personnel with application development responsibilities participate in industry-specific training.	<p>Interviewed the Manager of Security and IT Compliance and determined that developers are educated on Payment Card Industry Digital Security Standards (PCI DSS); the team stays updated on the Open Worldwide Application Security Project (OWASP) Top 10 list and uses security testing tools when necessary; and all developers are provided annual security awareness training based on OWASP content, which is provided through Inspired eLearning LMS</p> <p>Observed completion roster for Inspired eLearning and verified that developers completed the relevant training</p>	No Relevant Exceptions Noted
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	Performance evaluations and reviews are completed on a regular basis to ensure expectations are being met.	<p>Interviewed the People Business & Operations Partner and determined that ongoing one-on-ones with managers on a frequency established by the employee and manager; coaching between employees and leadership when performance expectations are not being met (January and July); and salary reviews are performed annually (February for North America and March for Europe)</p> <p>Observed the use of BambooHR to manage employees and verified that BambooHR captures the performance evaluation process</p>	No Relevant Exceptions Noted

Common Criteria for the Privacy Category			
Communication and Information			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	The organization has monitoring activities in place to ensure operational quality and control.	<p>Interviewed the Manager of Security and IT Compliance and determined that operational quality and control is managed through site reliability management (SRM) principles, which create a framework for the observability of IT systems and the related incident or service management processes and metrics to monitor the service; the SRM is responsible for establishing reliability expectations for all other engineering teams to follow, including internal service-level agreements (SLAs) (99.9%); in some cases, SLAs can also be committed to external customers, but this is not the default</p> <p>Observed Jira tickets from operational errors experienced in the production environment and verified tickets are used in response to application failures, which led to diminished performance, including failed payment processing functions</p> <p>Observed the use of Datadog and verified that it is used to monitor various services within the production application and to notify operations staff via PagerDuty</p> <p>Observed use of the SRM dashboards through Datadog to monitor site performance and verified that the following metrics are monitored:</p> <ul style="list-style-type: none"> Transaction and order processing metrics with a focus on credit card processing metrics tracking the number of transactions, including both successful and unsuccessful 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> Platform reliability (site reliability) metrics, which track platform availability across the PayByPhone technology components 	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	Leadership maintains continuous communication with employees, including meetings and emails, to ensure employees are aware of the tone and direction of the company.	<p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> The organization conducts monthly business update meetings, conducts weekly all-hands meeting, distributes weekly development and product news emails, and holds development and product quarterly townhall meetings The organization conducts quarterly leadership reviews with the management board (CEO, CTO, and CFO), conducts quarterly development townhall meetings, completes monthly business update reports, and conducts weekly one-on-one meetings between Compliance and the CISO & Senior Director of Reliability <p>Observed Teams invites for Friday meetings and verified that development and production leader meetings occur weekly</p> <p>Observed an email that was distributed to all staff (dated December 2022) and verified that all-hands meetings are conducted quarterly</p> <p>Observed a Teams invite for the monthly Global Leadership Forum (dated April 3, 2023) and verified that the organization conducts monthly leadership meetings</p> <p>Observed all-hands meeting materials and verified that key messages are</p>	No Relevant Exceptions Noted

		<p>delivered from the leadership to all employees</p> <p>Observed all-hands meeting materials for developers and production personnel and verified that platform engineering and operations personnel are informed of key messages as they relate to the specific duties</p> <p>Observed an email that addressed management team updates (dated January 19, 2023) and verified that it communicated personnel changes to the company</p>	
CC2.2.2	<p>The organization maintains formally documented incident response procedures that define the roles and responsible for personnel when handling incidents.</p>	<p>Reviewed the Incident Response document and verified that the primary goal of the incident management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations; the plan addresses the roles and responsibilities of the business user, the on-call engineer, SRM, and InfoSec (SecOps)</p> <p>Reviewed the Security Incident Response Policy and verified that it outlines requirements, policy statements, and initial process for reporting and responding to security events, specifically for PayByPhone information systems and operational procedures; the policy includes a comprehensive list of response team name, contacts, and responsibilities:</p> <ul style="list-style-type: none"> • Security Incident Response • Architecture Delegate • Platform Infrastructure Delegate • IT Compliance Manager • Legal Counsel, Compliance • Data Protection <p>Interviewed the Manager of Security and IT Compliance and determined that the core incident response team consists of Security and Compliance Team members and senior technical leadership; the team is responsible for</p>	<p>No Relevant Exceptions Noted</p>

		<p>both security as well as platform availability incidents</p> <p>Observed that the incident response commanders are also part of the SYS911 platform response team and verified that the Security team provides security incident response support as needed based on the type of incident, and the incident response teams also consist of other technical expertise as needed based on the type of the incident</p> <p>Observed that security incident response training is provided for the Security and Compliance team members and verified Udemy course completion certificates for the following:</p> <ul style="list-style-type: none"> • Manager of Security and IT Compliance • Information Security Analyst • Information Security Lead 	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	<p>The organization has a process for communicating incidents to impacted personnel and clients.</p>	<p>Reviewed the Ongoing Outage Response Guide and verified that it addresses the following steps for reporting incidents:</p> <ul style="list-style-type: none"> • Step 1: Impact Analysis • Step 2: Escalation • Step 3: Root Cause Analysis • Step 4: Communication • Step 5: Remediation • Step 6: “All Clear” Communication • Step 7: Next Steps <p>Reviewed the Ongoing Outage Response Guide and verified that it outlines the steps for reporting incident steps and communicating the impact of the incident with relevant people</p> <p>Observed the PayByPhone status page and verified that it includes a live status update for PayByPhone systems</p>	<p>No Relevant Exceptions Noted</p>

CC2.3.2	Contractual materials are used to communicate descriptions of services to the organization's clients.	<p>Observed three contracts and verified that the contracts include the following:</p> <ul style="list-style-type: none"> • Intellectual property rights • Definition and responsibilities pertaining to client data • Definition and responsibilities pertaining to customer (parker) data • Mutual indemnification • Mutual confidentiality and non-disclosure • Survival of specific clauses in the event of contract termination (specifically, confidentiality, intellectual property, and indemnification clauses) • PayByPhone responsibility to maintain PCI DSS compliance 	No Relevant Exceptions Noted
---------	---	--	------------------------------

Common Criteria for the Privacy Category

Risk Assessment

Ctrl #	Description of Controls	Service Auditor’s Tests of Controls	Test Results
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	The organization adheres to regulatory measures that impact its operations.	<p>Reviewed the Data Protection Policy and verified that it establishes the organization’s process of managing the availability, usability, integrity, and security of the data in enterprise systems in accordance with all legal, regulatory, compliance, and business requirements</p> <p>Interviewed the Manager of Security and Compliance and determined that PayByPhone adheres to the following business and regulatory compliance requirements:</p> <ul style="list-style-type: none"> • Canadian PIPEDA • Canadian Consumer Privacy Protection Act (CPPA) • European Union GDPR • PCI DSS • California Consumer Privacy Act (CCPA) 	No Relevant Exceptions Noted
CC3.1.2	The organization maintains policies and procedures for addressing a customer’s privacy rights.	<p>Reviewed the Guideline for Analyzing and Reporting a Data Breach to the Authorities and Data Subjects document and verified that it outlines the handling or notification of appropriate stakeholders in the event of a data breach necessary to comply with the GDPR requirements</p> <p>Reviewed the Data Protection Impact Assessment (DPIA) Process (dated May 2021) and verified that the DPIA is an important component of the risk-oriented approach in data protection; a DPIA is conducted to ensure that targeted measures can be found to contain risk</p> <p>Observed the organization’s online Privacy Policy located on the company website and verified that it addresses</p>	No Relevant Exceptions Noted

		data subjects rights under the GDPR and CCPA	
CC3.1.3	The organization conducts an annual risk assessment based on specified company objectives.	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that the Systems Group and the IT Operations (ITOPS) team does the following:</p> <ul style="list-style-type: none"> • Conducts an annual formal risk assessments to identify new threats and vulnerabilities • Informs the company about information security issues and vulnerabilities • Monitor and identifies new security vulnerabilities and assigns risk ranks to them <p>Interviewed the Manager of Security and IT Compliance and determined that the Compliance team reviews all risks monthly</p> <p>Interviewed the Manager of Security and Compliance and determined the following:</p> <ul style="list-style-type: none"> • At least annually, the organization coordinates a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks • Security risk assessments are reported and are shared with the Board on a quarterly basis • Vulnerabilities are assigned a risk ranking, and the risks levels include “high risk” and “critical” • The organization uses the Jira enterprise risk management (ERM) tool to track all risks in the risk register • Both enterprise risks and IT risks are tracked • Each risk is tracked separately and includes a description of the risk, risk category, likelihood, impact, risk type, and risk owner • New risks are provided to the Compliance team or IT Security 	No Relevant Exceptions Noted

		<p>team through leaders of other teams</p> <ul style="list-style-type: none"> • The Compliance team and the IT Security team meet monthly to discuss new risks and review old ones in the Jira ERM register • National Institute of Standards and Technology (NIST) 800-30 methodology is followed <p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p> <p>Observed the use of Jira IT assets and verified that it is used to track all assets such as Amazon Web Services (AWS) accounts, Elastic Container Service (ECS) clusters, and databases used within the system</p> <p>Observed the Jira ERM risk tickets and verified that legal, compliance, and IT risks are followed</p> <p>Observed the Q2 2023 risk register results and verified that the risk register is maintained and includes updates for resolved risks, newly identified risks, and current risks</p>	
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
CC3.2.1	The organization tracks and ranks enterprise and IT risks based on likelihood and impact.	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that the Systems Group and ITOPS team conducts an annual formal risk assessments to identify new threats and vulnerabilities</p> <p>Interviewed the Manager of Security and IT Compliance and determined that the Compliance team reviews all risks monthly</p> <p>Interviewed the Manager of Security and Compliance and determined the following:</p> <ul style="list-style-type: none"> • Both enterprise risks and IT risks are tracked 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Vulnerabilities are assigned a risk ranking, and the risks levels include “high risk” and “critical” • Each risk is tracked separately and includes a description of the risk, risk category, likelihood, impact, risk type, and risk owner <p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p>	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	Risks relating to fraud are assessed as part of the annual risk assessment.	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that a risk assessment is required to be performed at least annually</p> <p>Interviewed the Manager of Security and IT Compliance and determined that the Compliance team reviews all risks monthly</p> <p>Observed that rate limiting and geo-IP controls have been implemented through Apigee as a method to limit the risk of SMS and parking renewal bot fraud executed by external attackers against the system</p> <p>Observed the use of Terraform and AWS Guardrails and verified that they prevent misusing AWS account resources for unintended purposes</p> <p>Observed Backoffice databases capture all events involving creating, reading, updating, and deleting application records through Backoffice, which mitigates the risk of fraud through changing the Merchant of Record information for client parking transactions</p> <p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p>	No Relevant Exceptions Noted

		Observed the risk register from Q2-2023 and verified that examples of risks pertaining to fraud were captured in the register	
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	The organization performs a risk assessment following any significant changes to the environment.	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that the Systems Group and ITOPS team performs risk assessments when significant changes occur in the environment</p> <p>Interviewed the Manager of Security and IT Compliance and determined that the Compliance team reviews all risks monthly</p> <p>Interviewed the Manager of Security and Compliance and determined that risk assessments are performed upon significant changes to the environment</p> <p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p>	No Relevant Exceptions Noted

Common Criteria for the Privacy Category			
Monitoring Activities			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC4.1.1	The organization undergoes regulatory audits annually.	<p>Interviewed the Manager of Security and IT Compliance and determined that SOC 2 and PCI audits are performed by KirkpatrickPrice</p> <p>Observed completed SOC 2 and PCI reports and verified that the organization undergoes annual audits</p>	No Relevant Exceptions Noted
CC4.1.2	Risks are evaluated to determine the effectiveness of selected internal controls.	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that the Systems Group and ITOPS team does the following:</p> <ul style="list-style-type: none"> • Conducts an annual formal risk assessments to identify new threats and vulnerabilities • Informs the company about information security issues and vulnerabilities • Monitors and identifies new security vulnerabilities and assigns risk ranking to them • Uses reputable outside sources for vulnerability information • Subscribes to vendor and security-specific internet mailing lists for threat identification • Maintains updates and patches for operating systems and applications <p>Interviewed the Manager of Security and Compliance and determined the following:</p> <ul style="list-style-type: none"> • At least annually, the organization coordinates a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks • Security risk assessments are reported and are shared with the Board on a quarterly basis 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Vulnerabilities are assigned a risk ranking, and the risks levels include “high risk” and “critical” • The Compliance team reviews all risks monthly <p>Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023</p>	
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
CC4.2.1	Monitoring and alerting tools are installed to detect and notify staff of internal deficiencies.	<p>Observed Jira tickets from operational errors experienced in the production environment and verified that the tickets were filed in response to application failures which led to diminished performance, including failed payment processing functions</p> <p>Observed the use of Datadog and verified it is used to monitor various services within the production application and to notify operations staff via PagerDuty</p>	No Relevant Exceptions Noted
CC4.2.2	The relevant teams conduct regular meetings to discuss risk rankings and mitigation strategies.	<p>Interviewed the Manager of Security and Compliance and determined the following:</p> <ul style="list-style-type: none"> • Security risk assessments are reported and are shared with the Board on a quarterly basis • The Compliance team and IT Security team meet monthly to discuss new risks and review old ones in the Jira ERM register • The Compliance team reviews all risks monthly <p>Observed risk meeting minutes and verified that semi-monthly updates have occurred since December 2022 and most recent September 7, 2023; the meeting discussion topics include a review of new risks, a review of top risks, and a review of quarter security report</p>	No Relevant Exceptions Noted

Common Criteria for the Privacy Category			
Control Activities			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	The organization maintains a formally documented Security Awareness and Acceptable Use Policy that outlines the guidelines for users who use company assets.	<p>Reviewed the Security Awareness and Acceptable Use Policy and verified that it includes provisions for end-user use of PayByPhone assets; it defines prohibited actions pertaining to PayByPhone data and systems; it defines critical technologies to include internet, intranet, and extranet-related systems, including computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and File Transfer Protocol (FTP)</p> <p>Interviewed the Manager of Security and IT Compliance and the People Business & Operations Partner and determined that all personnel must acknowledge the policy as part of the overall PayByPhone policy set upon new hire</p> <p>Observed onboarding records for a sample of new hires (4 of 44) and verified that new hires review and acknowledge policies</p>	No Relevant Exceptions Noted
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	The Systems Groups maintain the formally documented Information Security Policies and Procedures that define general control activities over technology.	<p>Reviewed the Information Security Policies and Procedures is a single, comprehensive information security policy covering a range of topics, each in their own top-level section; topics include:</p> <ul style="list-style-type: none"> • Roles and responsibilities for managing the information security program • Change management • Data classification and control • Background checks • Data retention and disposal • Paper and electronic media 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Firewall, router, and switch security administration • Configuration management • Antivirus • Backups • Encryption of data at rest and in transit • Software development and lifecycle management • Incident response • Employee identification • Logging controls • Service providers and third parties • Detecting failures of critical security controls • Internal audit of security controls • Security awareness • System configuration standards <p>Interviewed the Manager of Security and IT Compliance, the Information Security Lead, the CISO & Senior Director of Reliability, and the Information Security Analyst and determined the following:</p> <ul style="list-style-type: none"> • The Systems Groups, including Cloud Platforms and Corporate IT, are responsible for detailed policies and procedures as well as implementing controls on information systems, reviewing relevant information security logs, and administering user accounts, among other responsibilities • Users are responsible for understanding the consequences of their actions, maintaining awareness of policies, attending security awareness training, and remaining knowledgeable of data classification and handling requirements <p>Observed Confluence and verified that it is used to distribute information security policies to all parties</p> <p>Observed onboarding records for a sample of new hires (4 of 44) and</p>	
--	--	--	--

		verified that new hires review and acknowledge policies	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	The organization has a process for continuously reviewing and updating the Information Security Policies and Procedures.	<p>Interviewed the Manager of Security and IT Compliance and determined that the Security team is responsible for creating and updating policies, and management is responsible for policy approval</p> <p>Interviewed the Manager of Security and IT Compliance, the Information Security Lead, the CISO & Senior Director of Reliability, and the Information Security Analyst and determined the following:</p> <ul style="list-style-type: none"> • The organization has a monolithic information security policy that includes an internal review and approval • PayByPhone maintains an information security policy in Jira as Information Security Policies and Procedures • As a Jira-based document, it is continuously updated as needed; the CTO, or their designee, is responsible for managing the information security policy; and in practice, this responsibility is assigned to the CISO and primarily executed by the Manager, Security and IT Compliance • The policy is reviewed annually by the M-Board before incorporating into the Global Organization Handbook <p>Observed at least eight minor policy updates that were made within the audit period and verified that the policies and procedures are continuously updated</p> <p>Observed Confluence and verified that it is used to distribute information security policies to all parties</p>	No Relevant Exceptions Noted

Common Criteria for the Privacy Category

Logical and Physical Access Controls

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
CC6.1.1	The organization has tools in place to authenticate user access to the cloud infrastructure.	<p>Reviewed the Information Security Policies and Procedures and verified that authentication is implemented for all systems and databases containing cardholder information, limiting direct SQL queries to administrators</p> <p>Observed all user identities are implemented in Azure Active Directory and that Volkswagen Financial Service (VWFS) has built and maintains Bifrost, which is a SAML-based interface for integration into all supported cloud portals used within Volkswagen, and verified that PayByPhone currently uses Bifrost for access to AWS Console; therefore, the authentication hierarchy when an administrator needs to access the AWS Console is as follows: AWS Console – > Bifrost –> Azure Active Directory where all identities are derived from Azure Active Directory</p> <p>Observed SAML integration configurations for Bifrost, Azure Active Directory, AWS Console, and Google Cloud and verified that all access to any in-scope system component is provided exclusively through the user's Azure Active Directory credentials</p> <p>Observed that elevated access is managed through a just-in-time provisioning system in Bifrost; an engineer with the ability to request elevated access must submit firefighter request, which is approved by another person on the authorized approvers list, after which the access is granted on a temporary, time-bound basis</p>	No Relevant Exceptions Noted

		<p>Observed the firefighter log and verified that all firefighter access requests are logged</p> <p>Observed the use of the firefighter access feature in Bifrost to grant just-in-time access to cloud system administrator</p>	
CC6.1.2	The organization has tools in place to authenticate user access to the Backoffice portal.	<p>Interviewed the Manager of Security and IT Compliance and determined that authentication is mandated for all user IDs, system accounts, and application accounts through passwords</p> <p>Observed the Backoffice application and verified that it defines its own users and stores user credentials within the application databases using the bcrypt adaptive hashing algorithm</p> <p>Observed user accounts for the Backoffice application and verified that accounts are hashed using bcrypt prior to storage in the application database</p> <p>Observed application configuration settings and verified that bcrypt is used with a cost factor of 12, a system-specific pepper and salt length of 16 bytes</p>	No Relevant Exceptions Noted
CC6.1.3	All users are assigned a unique user ID prior to accessing system components.	<p>Interviewed the Manager of Security and IT Compliance and determined that unique user IDs are formed by combining the employee’s first initial with their last name</p> <p>Observed that Azure Active Directory is used for integrated authentication to all infrastructure, including cloud-based applications and cloud service provider platforms, and to all user laptops including both Windows and MacOS devices</p>	No Relevant Exceptions Noted
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For		

those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	<p>Access rights and privileges are provisioned to new hires and contractors based on their job role.</p>	<p>Reviewed the Information Security Policies and Procedures and verified that access to data is assigned based on least privilege; System Group approves access authorization based on an employee’s job classification and function; a member of the Systems Group must review the Access Authorization Form to assure proper separation of duties; and contractor accounts require Systems Group approval and should automatically expire at the end of the contract</p> <p>Observed a demonstration of Azure Active Directory role assignments for user accounts and verified that those ending in “-SA” are exclusively assigned to Azure Active Directory roles</p> <p>Observed Jira tickets for a sample of new hires (4 of 44) and verified that Jira tickets include approval prior to implementation</p> <p>Observed access requests to Azure Active Directory group permissions and verified that provisioned access is consistent with documented approvals</p> <p>Observed roles for general users, system administration, and other purposes are defined in the Access Control Matrix in the Information Security Policies and Procedures Jira page and verified that the Access Control Matrix includes the following defined roles:</p> <ul style="list-style-type: none"> • Basic User • Support • Manager • Developer • System Administrator • Security Administrator 	No Relevant Exceptions Noted

<p>CC6.2.2</p>	<p>The organization has a process for managing passwords, including resetting passwords and assigning first-time passwords.</p>	<p>Reviewed the Demonstrate Password Reset Procedures document and verified that the reset password process is completed in Microsoft Azure</p> <p>Interviewed the Manager of Security and IT Compliance and determined the following regarding password resets:</p> <ul style="list-style-type: none"> • System Administrators must validate the identity of users before performing a password reset • Passwords are set by System Administrators and must be changed by the user immediately upon the user's next login • System Administrators must set initial passwords that are unique and compliant with the password rules <p>Observed the use of the LastPass password generator to assign a randomly generated password to new user accounts and when an administrator is asked to reset a user's password</p> <p>Observed new user account passwords and verified that password reset requests use a randomly generated password</p> <p>Observed the use of first-time passwords and password reset requests and verified that both use randomly assigned passwords</p> <p>Observed system administrators through the first-time password and password reset processes and verified that random passwords are created using LastPass' password generator feature</p>	<p>No Relevant Exceptions Noted</p>
<p>CC6.2.3</p>	<p>The organization uses Azure Active Directory to enforce password composition requirements for employees.</p>	<p>Reviewed Information Security Policies and Procedures (dated July 11, 2023) and verified that user authentication procedures require unique user accounts, passwords or</p>	<p>No Relevant Exceptions Noted</p>

		<p>token entry, and acknowledgement of security policies, and passwords are at least 12 characters long, complex, and changed every 90 days</p> <p>Observed that all password policies are enforced in Azure Active Directory and include minimum password length, expiry, complexity, and reuse provisions:</p> <ul style="list-style-type: none"> • Minimum password length is eight-character passwords (PayByPhone policy requires 12 characters, but Azure Active Directory is limited to eight) • Passwords consist of a combination of uppercase and lowercase characters • Passwords cannot include family names, phone numbers, car registration numbers, company name, usernames, or birthdays • The previous four passwords are remembered and cannot be re-used • Passwords are changed every 90 days 	
CC6.2.4	<p>Clients are required to meet password composition standards when accessing Backoffice.</p>	<p>Reviewed the Information Security Policies and Procedures and verified that System Administrators set initial passwords that comply with password rules, and users must change them upon login; identity verification is required for password resets, using approved methods such as face-to-face or remote procedures</p> <p>Interviewed the Manager of Security and IT Compliance and determined that passwords adhere to the following standards:</p> <ul style="list-style-type: none"> • Standard passwords are minimum of 12 characters long • System Administrator passwords are minimum of 16 characters long • Passwords must contain a combination of numbers, 	<p>No Relevant Exceptions Noted</p>

		<p>uppercase letters, and lowercase letters</p> <ul style="list-style-type: none"> • The previous four passwords cannot be re-used • Passwords are updated every 90 days <p>Observed password settings in Backoffice and verified that the previous four passwords are remembered and cannot be re-used, and passwords must contain at least seven characters</p>	
CC6.2.5	Sessions are configured to timeout following a period of inactivity.	<p>Observed Microsoft Intune and Mosyle policies applied to all Windows and MacOS devices and verified that the screensaver locks after 10 minutes of inactivity, and a five-second grace period is applied within which the user will not be required to enter their password</p> <p>Observed that the timeout policy is enforced on end-user devices and verified that the policies are enforced</p>	No Relevant Exceptions Noted
CC6.2.6	Accounts are configured to lock for 30 minutes following six invalid login attempts.	<p>Interviewed the Manager of Security and IT Compliance and determined that user accounts are locked out after six invalid login attempts and for a duration of 30 minutes</p> <p>Observed Azure Active Directory lockout settings and verified that accounts are locked out for 30 minutes after six invalid login attempts</p>	No Relevant Exceptions Noted
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
CC6.3.1	The organization has a process for temporarily assigning elevated access to users following administrator approval.	<p>Reviewed the Information Security Policies and Procedures and verified that System Group approves access authorization based on an employee's job classification and function; a member of the Systems Group must review the Access Authorization Form to assure proper separation of duties; and contractor accounts require</p>	No Relevant Exceptions Noted

		<p>Systems Group approval and automatically expire at the end of the contract</p> <p>Observed that no users have permanent, read-write administrative access to the AWS Console and verified that when a PayByPhone employee needs elevated access to the AWS Console, they log into Bifrost and request elevated access, including with a time limit; another administrator on the approval list must approve the request, after which the requestor is granted elevated access to the AWS Console; when the time limit has expired, the requestor's access is automatically demoted to the prior access level; this is referred to as firefighter access, which is an example of just-in-time access management</p>	
CC6.3.2	Access is revoked for terminated employees, and the organization has a process for removing inactive accounts.	<p>Reviewed the Information Security Policies and Procedures and verified that access is revoked immediately for terminated, transferred, or unnecessary users, and user IDs are disabled after 90 days of inactivity and purged after an additional 30 days</p> <p>Observed offboarding records for a sample of terminated users (9 of 93) and verified that the employees were removed from all relevant systems, including BambooHR, Azure Active Directory, and Backoffice</p>	No Relevant Exceptions Noted
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	The organization implements mobile device management (MDM) processes to ensure that remote users have their devices protected.	Reviewed the Mobile Device Management Policy within the Information Security Policies and Procedures and verified that all company end-user devices are required to use desktop firewalls and connect using Zero Trust Network Access (ZTNA) solutions provided by the company, and the policy includes requirements for personal firewalls and use of the Zscaler Zero Trust Network	No Relevant Exceptions Noted

		<p>Access solution for remote access to company applications</p> <p>Interviewed the Manager of Security and IT Compliance and CISO & Senior Director of Reliability and determined that an inventory of company assets is maintained; all end-user devices are managed through MDM platforms as follows:</p> <ul style="list-style-type: none"> • Windows devices: Microsoft Intune • MacOS devices: Mosyle Enhanced Apple Device Management <p>Observed use of Intune (Windows) and Mosyle (MacOS) MDM platforms and verified that they are used to manage configurations for end-user devices</p> <p>Observed that PayByPhone has implemented end-user device safeguards and verified that each employee-assigned device presents its own security perimeter; critical elements of these end-point controls include:</p> <ul style="list-style-type: none"> • Centrally managed MDM using Microsoft Intune for Windows devices and Mosyle for MacOS • ZTNA using Zscaler • Centralized identity management using Azure Active Directory 	
CC6.4.2	AWS is responsible for protecting the data it houses on behalf of PayByPhone.	Observed that the organization obtained a SOC 2 audit report for AWS and verified that all critical systems and applications are located in AWS, which is responsible for physically protecting the data it holds; interested parties should review the subservice organization’s audit report	No Relevant Exceptions Noted
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.		

<p>CC6.5.1</p>	<p>The organization has a process for physically destroying assets and data.</p>	<p>Reviewed the Disposal Policy and verified that the following are enforced:</p> <ul style="list-style-type: none"> • Hard disks are sanitized using s National Institute of Standards and Technology (NIST) 800-88 standard degauss or crosscut shred to, or by penetrating the disk platters with one or more half inch holes drilled though them • Floppy disks are disintegrated, incinerated, pulverized, crosscut shred, or melted • Tape media are degaussed, crosscut shred, incinerated, pulverized, or melted • USB thumb drives, smart cards, and digital media are incinerated, pulverize, or melted • Optical disks (CDs and DVDs) are destroyed, incinerated, pulverized, crosscut shred, or melted • Before computer or communications equipment can be sent to a vendor for trade-in, servicing or disposal, all cardholder data must be destroyed or removed according to the approved methods • Removable computer storage media such as floppy, optical disks, or magnetic tapes may not be donated to charity or otherwise recycled • Outsourced destruction of media containing cardholder data must use a bonded disposal vendor that provides a Certificate of Destruction <p>Observed a completed Certificate of Destruction from DataKnox.io and verified that data was destroyed in accordance with NIST 800-53</p> <p>Observed a completed Certificate of Destruction from Infoshred and</p>	<p>No Relevant Exceptions Noted</p>
----------------	--	--	-------------------------------------

		verified that third parties are used to destroy data	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	Source code is reviewed prior to each change and is stored in GitLab and GitHub.	<p>Reviewed the Technical Standards and Policies documentation and verified that source code is stored in GitLab and GitHub, which uses Active Directory for authentication and authorization</p> <p>Reviewed the Code Review document and verified that the following are addressed:</p> <ul style="list-style-type: none"> • Code reviews are required for every code change • Reviewers must confirm that the reviewed code is free from security defects • A GitLab merge request is required for each code review • Merge requests should have at least one reviewer • For services deployed in the cardholder data environment, a Security Review confirmation is needed from at least one reviewer • Tickets are reviewed before deployments can be approved <p>Interviewed the Manager of Security and IT Compliance and CISO & Senior Director of Reliability and determined that the Terraform code is maintained in PayByPhone’s GitLab source code management repositories; developers have access to the source code repository (GitLab and GitHub)</p> <p>Observed that source code is stored in GitLab and GitHub and verified that authentication and authorization is managed using Active Directory</p> <p>Observed the use of GitLab and verified that Terraform is used to manage source code</p>	No Relevant Exceptions Noted

<p>CC6.6.2</p>	<p>The organization has a process for encrypting passwords during transmission and storage.</p>	<p>Observed the Backoffice password hash settings and verified that the Backoffice portal uses bcrypt for password hashing</p> <p>Observed that PayByPhone uses a cloud-based solution called Microsoft Azure Active Directory for authentication and verified that Microsoft handles the transmission of these passwords</p> <p>Observed access to infrastructure components and verified that access is provided through Azure Active Directory-integrated single sign-on</p> <p>Observed Azure Active Directory authentications and verified that they occur using Transport Layer Security (TLS) encrypted sessions under Microsoft management</p>	<p>No Relevant Exceptions Noted</p>
<p>CC6.6.3</p>	<p>Multi-factor authentication (MFA) is used for remote access to the organization’s corporate networks.</p>	<p>Reviewed Information Security Policies and Procedures (dated July 11, 2023) and verified that critical systems with access to the cardholder data environment should have two-factor authentication</p> <p>Interviewed the Information Security Lead and determined that the organization has implemented two distinct Azure Active Directory conditional access policies; the policies necessitate the use of MFA during login attempts, reinforcing the authentication process with an additional layer of identity verification</p> <p>Observed the use of Microsoft Authentication and verified that it is used for the MFA solution</p> <p>Observed the use of Zscaler to provide remote network access to the in-scope AWS accounts and virtual private clouds (VPCs) and verified that Zscaler authentication is integrated with Azure Active Directory, which</p>	<p>No Relevant Exceptions Noted</p>

		<p>requires MFA for all authentication requests regardless of application</p> <p>Observed that all accounts require the use of MFA and verified that MFA is implemented in Azure Active Directory; two Azure Active Directory conditional access policies have been implemented regarding MFA:</p> <ul style="list-style-type: none"> • “RequireMFA-MSAuth,” is designed for all users across the organization; this policy necessitates the use of MFA during login attempts for access to any PayByPhone Azure Active Directory-integrated application • “1 day sign-in frequency for admins,” specifically targets administrative users within the system; this policy mandates that administrators not only provide their password but also undergo MFA verification daily 	
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.		
CC6.7.1	<p>Sensitive data is secured any time it must be transmitted or received via open, public networks.</p>	<p>Interviewed the Manager of Security and IT Compliance and determined that all databases are encrypted by default by AWS Guardrails</p> <p>Observed cipher suite components and verified that they provide strong security</p> <p>Observed cryptography configurations for application programming interface (APIs) and application and verified that the configurations only receive traffic on TLS ports (TCP/443) in communication between all system components, and that TLS 1.2 is supported, and that strong cipher suite selections are supported including:</p> <ul style="list-style-type: none"> • Key exchanges supporting perfect forward secrecy with key lengths of 2048+ (FFC) and 256+ (elliptic curve) 	<p>No Relevant Exceptions Noted</p>

		<ul style="list-style-type: none"> • RSA host authentication with key lengths of 2048+ • AES128, AES256 and ChaCha20 bulk encryption SHA256 or stronger MAC <p>Observed that HTTP Strict Transport Security (HSTS) is required for all communications and verified that communication is delivered to all browsers that attempt to connect on HTTP</p> <p>Observed the encryption of sensitive data at rest and verified that encryption of PII is accomplished through AWS RDS-based encryption using an encryption key managed in AWS Key Management Service (KMS); encryption of cardholder data (CHD) is performed by the application using a custom-built application component that uses AWS-provided software development kits (SDKs) to interface with AWS KMS; and each data element is encrypted its own KMS-managed encryption key and stored in the database as encrypted content</p> <p>Observed encryption of data in transit and verified that all web application user interfaces and application programming interfaces use HTTPS based on TLS 1.2 and strong cipher suites</p>	
CC6.7.2	The organization uses AWS and Terraform to manage encryption keys.	<p>Reviewed the Cardholder Data Encryption Policy (dated August 17, 2023) and verified the following:</p> <ul style="list-style-type: none"> • Key management for cardholder data encryption keys is completed through Terraform in the terraform-encryption-keys-live repository • Access to encryption keys is managed by submitting a ticket to the Security and Compliance Service Desk • PII data is encrypted using AWS-provided capabilities for database 	No Relevant Exceptions Noted

		<p>encryption through the RDS service</p> <ul style="list-style-type: none"> • Encryption keys are managed through the AWS KMS <p>Interviewed the Manager of Security and IT Compliance and determined that AWS is responsible for key management</p> <p>Observed the use of AWS KMS and verified that it is used manage all encryption keys for sensitive data at rest</p> <p>Observed that encryption keys are retained in an AWS account and verified that it provides additional protection for KMS-related functions to restrict team member access unless a specific need exists to interact with KMS</p> <p>Observed the use of key management and verified that all key-encrypting keys are retained in AWS KMS, all data-encrypting keys are generated by AWS KMS, key-encrypting keys are automatically rotated on an annual basis, and encryption keys are retained in an isolated AWS account to provide additional access control for team members that can interact with the KMS</p> <p>Observed the effect of encryption on application data stored in DynamoDB and verified that the encrypted data is written to the database along with the necessary “encryption context” data for KMS to provide the plaintext key for future decryption operations</p> <p>Observed all other sensitive data is encrypted by AWS RDS-provided encryption features</p> <p>Observed RDS configurations and verified that encryption is enabled for</p>	
--	--	---	--

		each database instance that contains PII or other sensitive data	
CC6.7.3	The organization’s development, integration, consolidation, and production environments are unique environments that are logically separated, and the separation of duties are enforced throughout application development.	<p>Reviewed the Tenant Environments document and verified that the following are addressed:</p> <ul style="list-style-type: none"> • PayByPhone uses four environments as part of its SDLC: development, integration, consolidation, and production • Each environment is completely isolated and there is no connectivity between environments • Lowest level environments (development and integration) do not have outbound internet connectivity • Services in development and integration are not reachable from the internet without proper authentication • Development is unstable and meant to be used for experimentation • Consolidation access mimic the production environment in terms of network flow, access, IAM roles, and whitelisted AWS services <p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> • Personnel may be granted role-based access to the pre-production environments in order for users to perform job duties; however, access to production environments is only granted on a just-in-time, time-limited basis with explicit approval using the firefighter access request process • Tasks related to coding, testing, and maintaining the production environment are separated and the company establishes a barrier between development project teams and the production environment 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> User stories are written and security requirements are established by the product management team; the development team and solutions architect shape the security requirements during the story-writing process The production personnel do not write code and test software, but they maintain the production environment and make sure there is a barrier between project teams and the production environment <p>Observed a screenshot showing personnel access to the pre-production environments for the multi-domain tenant and verified that there is no nominal access to the production environment</p> <p>Observed separation of production and non-production environments (development, integration-testing, and consolidation) through distinct AWS accounts and verified that there exist no network connections between prod and non-prod accounts and resources</p>	
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.		
CC6.8.1	Antivirus is installed on all removable media and end-user endpoints to detect and prevent the intrusion of malicious software.	<p>Interviewed the Manager of Security and IT Compliance and determined that antivirus is used on all end-user endpoints; as all production application workloads are based on Docker containers, antivirus is managed by AWS on the underlying infrastructure</p> <p>Observed use of Microsoft Defender antivirus as managed through Microsoft Intune and verified that Intune enforces the use of Defender for all Intune-managed devices, including both Windows and MacOS operating systems</p>	No Relevant Exceptions Noted

		Observed the use of Microsoft Defender antivirus and verified that Microsoft Defender is configured to scan all removable media for potential malware, and it is configured to receive daily updates	
--	--	--	--

Common Criteria for the Privacy Category

System Operations

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
CC7.1.1	<p>Web application testing and sprints are used to ensure that applications are not susceptible to common vulnerabilities.</p>	<p>Reviewed the Vulnerability Management Policy within the Information Security Policies and Procedures and verified the following:</p> <ul style="list-style-type: none"> • Public-facing web applications are required to be reviewed, and that all vulnerabilities identified are required to be corrected; the application is to be re-evaluated after the corrections have been made • The organization implements application vulnerability management practices to identify and prevent common web application vulnerabilities <p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> • Starting with writing user stories, security requirements are established by the product management team • As part of writing user stories, the development team and the solutions architect are involved in shaping the security requirements • Once the stories are planned into a sprint, the development team implements and tests the story • PayByPhone follows a test-driven development (TDD) approach, ensuring that if the security requirement can be proven via a unit or integration test it will be, even before the implementation code change is made • If it cannot be tested with a unit or integration test, then it is tested manually, potentially with 	Exception Noted

		<p>security testing tools, before it is marked as complete</p> <ul style="list-style-type: none"> • TDD is practiced, and regression tests are used to identify and fix security bugs • Dynamic analysis is performed on UI-based endpoints using the Tenable web application scanner <p>Observed reports from JFrog and verified that JFrog scanning is built into the continuous integration and continuous delivery (CI/CD) pipeline; the organization uses JFrog for scanning containers to be deployed in pre-production and production environments and also run Tenable scans on the production, development, quality assurance (QA), and test environments</p> <p>Observed Tenable.io vulnerability scans completed against all public-facing API and UI endpoints and verified that scans are completed approximately every 90 days</p> <p><i>Exception: As determined through a penetration test of the PayByPhone applications, the Backoffice application was vulnerable to a URL redirection weakness, which allowed bad actors to use the application to redirect users to websites of the actor's choosing. The auditor observed updated penetration testing results (October 2023) to confirm that each of these items were remedied.</i></p>	
CC7.1.2	Internal and external scans are conducted on a regular basis to identify potential vulnerabilities, which are prioritized and remediated based on severity.	<p>Reviewed the Vulnerability Management Policy within the Information Security Policies and Procedures and verified the following:</p> <ul style="list-style-type: none"> • The Systems Group is responsible for conducting internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule 	No Relevant Exceptions Noted

		<p>modifications, product upgrades), and the process includes identifying any unauthorized wireless devices on the network</p> <ul style="list-style-type: none"> • When internal vulnerability scans identify high-risk vulnerabilities, the issues must be remediated and rescans must be performed after remediation to verify that the high-risk vulnerabilities are resolved • Additional external vulnerability scans must be performed by a scan vendor qualified by the payment card industry at least quarterly; the results of each scan must satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities) • When external vulnerability scans identify vulnerabilities with a CVSS score of 4.0 or higher, the issues must be remediated and rescans must be performed after remediation to verify that the vulnerabilities are resolved <p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> • Docker containers are used throughout the production applications, and AWS ECR Container Image Scanning is performed when a new image is pushed to the repository and continuously on all images uploaded in the prior 30 days • Scans are performed on end-user devices using Microsoft Defender, and these scans are performed weekly against all user endpoints • Alerts are delivered to a Slack channel shared with operations teams and that vulnerability scans are conducted as follows 	
--	--	---	--

		<p>Observed ECR image scanning configuration and verified that it is enabled and actively identifies new vulnerabilities in existing images</p> <p>Observed the use of agent-based Microsoft Defender and verified that Microsoft Defender is used to conduct scanning on end-user devices</p> <p>Observed external vulnerability scans and verified that they are completed on a weekly basis</p>	
CC7.1.3	<p>The organization conducts application and network layer penetration testing annually and following significant changes to the network in order to identify and remediate weaknesses.</p>	<p>Reviewed the Vulnerability Management Policy within the Information Security Policies and Procedures and verified penetration tests at both the application and network layer must be performed annually or after any significant change in the network</p> <p>Interviewed the Information Security Lead and determined that penetration tests at both the application and network layer must be performed annually or after any significant change in the network; PayByPhone uses a security company who is qualified to perform internal as well as external penetration testing</p> <p>Observed the external application and network penetration test report (dated August 2023) and verified that the penetration tests cover external, internet-accessible systems and applications were completed by an external company specializing in penetration testing services</p> <p>Observed that penetration testing is performed by a third party specializing in penetration testing services and verified that penetration tests evaluate the security of infrastructure, and both user and API interfaces; exploitable vulnerabilities are identified, remediated, and retested to verify effective remediation</p>	<p>No Relevant Exceptions Noted</p>

		Observed penetration testing results and verified that that testing was performed by Mirai Security, penetration tests include infrastructure and application components, and exploitable vulnerabilities were retested after remediation	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity’s ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
CC7.2.1	Network monitoring and logging tools are installed to capture security events.	<p>Interviewed the Manager of Security and IT Compliance, the CISO & Senior Director of Reliability, and the Software Architect and determined the following:</p> <ul style="list-style-type: none"> • Security-related event logs are captured by the AWS, Bifrost, and Google Apigee cloud platforms • All actions taken against AWS-based assets are captured via AWS CloudTrail, written to a dedicated S3 bucket, and reviewed by CloudGuard • Logs are retained for at least one year to support forensic reviews in the case of a security incident <p>Observed use of AWS CloudTrail, CloudGuard, Slack, and PagerDuty and verified that they are used to collect, review, analyze, and provide relevant notifications pertaining to security events within the production infrastructure</p> <p>Observed Jira tickets from operational errors experienced in the production environment and verified tickets are used in response to application failures, which led to diminished performance, including failed payment processing functions</p> <p>Observed the use of Datadog and verified that it is used to monitor various services within the production</p>	No Relevant Exceptions Noted

		application and to notify operations staff via PagerDuty	
CC7.2.2	Intrusion detection and prevention tools are in place to detect anomalies and alerts are sent to personnel for remediation.	<p>Reviewed the Vulnerability Management Policy within the Information Security Policies and Procedures and verified that networks and systems that fall under payment card system scope must also be monitored by an intrusion detection or prevention system that alerts personnel of potential compromises</p> <p>Observed that GuardDuty is enabled on select AWS accounts and verified that the GuardDuty for the accounts are centrally managed by Managed Private Servers (MPS), who notifies PayByPhone if there are findings</p>	No Relevant Exceptions Noted
CC7.2.3	Logs are reviewed as part of daily security activities in order to detect and remediate suspicious activity.	<p>Interviewed the Manager of Security and IT Compliance, the Information Security Lead, and the Information Security Analyst and determined the following:</p> <ul style="list-style-type: none"> • Security logs are reviewed by automated log review tools to detect and notify operations personnel of potential security incidents • Check Point CloudGuard provides ongoing review and analysis of CloudTrail and other audit logs and provides notification through PagerDuty when suspicious activity is detected • The Security team performs a daily check of CloudGuard <p>Observed CloudTrail and CloudGuard configurations and verified that all relevant security events are reviewed daily</p> <p>Observed use of Slack channels, including the Sys911 channel, and verified that it is used to notify operations personnel of security anomalies, that each notification is presented as a thread in Slack, and that</p>	No Relevant Exceptions Noted

		follow-up was performed by relevant personnel and documented in each threaded item	
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
CC7.3.1	Security incidents are analyzed to determine appropriate remediation and prevention activities.	<p>Reviewed the Incident Response and verified that the following are addressed:</p> <ul style="list-style-type: none"> • Incident process • Post-incident process • Major incident process • Security incident process <p>Reviewed the Sys911 Incident Response and Resolution Procedure and verified that it includes a detailed process flow chart to follow in the event of a production alert</p> <p>Reviewed the Security Incident Response Policy and verified that it outlines requirements, policy statements, and initial process for reporting and responding to security events</p> <p>Interviewed the Manager of Security and IT Compliance and the CISO & Senior Director of Reliability and determined the following regarding availability and security incidents:</p> <ul style="list-style-type: none"> • If the incident is a single domain, then the incident is managed by the Service Platform team • If the incident is a multi-domain, then an incident commander is assigned, who coordinates the incident and updates the status page • As needed to resolve the incident, the incident command brings in additional resources and manages both internal and external communications <p>Observed Jira ticket for a recent incident regarding the unexpected</p>	No Relevant Exceptions Noted

		<p>discovery of CHD in an application log and verified the following:</p> <ul style="list-style-type: none"> • Communication strategies, roles, and responsibilities were implemented in the related Slack security alerts channel • The root cause of the incident was identified as .Net application code that added ApplePay device primary account numbers (DPANs) to Datadog application logs • .Net coding changes were observed to be implemented through an associated development ticket (UB-3640) • Data clean-up was observed in engineering tickets associated with the master ticket 	
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
CC7.4.1	<p>Incident response policies and procedures have been formally documented and implemented to define incident identification, reporting, containment, and remediation processes.</p>	<p>Reviewed the Incident Response and verified that the following are addressed:</p> <ul style="list-style-type: none"> • Incident process • Post-incident process • Major incident process • Security incident process <p>Reviewed the Sys911 Incident Response and Resolution Procedure and verified that it includes a detailed process flow chart to follow in the event of a production alert</p> <p>Reviewed the Security Incident Response Policy and verified that it outlines requirements, policy statements, and initial process for reporting and responding to security events</p> <p>Interviewed the Manager of Security and IT Compliance and the CISO & Senior Director of Reliability and determined and determined the following regarding availability and security incidents:</p>	<p>No Relevant Exceptions Noted</p>

		<ul style="list-style-type: none"> • If the incident is a single domain, then the incident is managed by the Service Platform team • If the incident is a multi-domain, then an incident commander is assigned, who coordinates the incident and updates the status page • As needed to resolve the incident, the incident command brings in additional resources and manages both internal and external communications <p>Observed Jira ticket for a recent incident regarding the unexpected discovery of CHD in an application log and verified the following:</p> <ul style="list-style-type: none"> • Communication strategies, roles, and responsibilities were implemented in the related Slack security alerts channel • The root cause of the incident was identified as .Net application code that added ApplePay DPANs to Datadog application logs • .Net coding changes were observed to be implemented through an associated development ticket (UB-3640) • Data clean-up was observed in engineering tickets associated with the master ticket 	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	Outside sources are reviewed to identify patches and new vulnerabilities that could impact the organization’s networks and systems, and patches are installed based on the criticality of the vulnerability.	<p>Reviewed the Vulnerability Management Policy within the Information Security Policies and Procedures and verified the following:</p> <ul style="list-style-type: none"> • All security patches, hot-fixes, and service packs identified by the Systems Group or the System Administrator must be installed on applicable systems within 30 days of vendor release and in accordance with change management processes 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Critical and high-ranking vulnerabilities are patched within 30 days • Medium and low vulnerabilities are patched within three months <p>Interviewed the Manager of Security and IT Compliance and the CISO & Senior Director of Reliability and determined the following:</p> <ul style="list-style-type: none"> • Members of the Systems Group must be informed of information security issues and vulnerabilities applicable to PayByPhone computing systems • When security issues are identified, the Systems Group is responsible for notifying appropriate personnel, including System Administrators • The primary method for identifying new threats is through vendor and security-specific internet mailing lists • The organization subscribes to NVD, Microsoft, AWS, and as well as other vendor lists applicable to PayByPhone-specific software packages and systems • New vulnerabilities are communicated through Slack and evaluated for impact on PayByPhone Technologies • New security vulnerabilities are required to be monitored and are assigned a risk ranking <p>Observed use of Slack and verified that it is used to receive and triage new vulnerabilities</p>	
CC7.5.2	The organization incorporates lessons learned from incident response activities into the incident response policies and procedures.	<p>Reviewed the Incident Response and verified that the post-incident process is addressed</p> <p>Interviewed the Manager of Security and IT Compliance and the CISO & Senior Director of Reliability and determined that once the incident is</p>	No Relevant Exceptions Noted

		<p>resolved, the team conducts a post-mortem exercise to identify the cause and improvements to prevent a recurrence</p> <p>Observed Jira ticket for a recent incident regarding the unexpected discovery of CHD in an application log and verified the following:</p> <ul style="list-style-type: none"> • Communication strategies, roles, and responsibilities were implemented in the related Slack security alerts channel • The root cause of the incident was identified as .Net application code that added ApplePay DPANs to Datadog application logs • .Net coding changes were observed to be implemented through an associated development ticket (UB-3640) • Data clean-up was observed in engineering tickets associated with the master ticket <p>Observed the master Security Incident Response ticket and verified that lessons learned from the incident are documented</p>	
--	--	---	--

Common Criteria for the Privacy Category

Change Management

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.1	Formal configuration standards are maintained for all systems in use within the environment, and systems are required to be configured appropriately prior to promotion to the production networks.	<p>Reviewed the Information Security Policies and Procedures document (dated August 7, 2023) and verified that all servers and network devices on PayByPhone networks, whether managed by employees or by third parties, are built and deployed in accordance with a system configuration policy; the following system build and deployment guidelines are enforced:</p> <ul style="list-style-type: none"> • Maintain a System Configuration Record for each deployed system, updating it with any modifications • Enforce file integrity monitoring (FIM) software for systems handling cardholder data • Install antivirus software on operating systems • Log, monitor, and review changes on critical systems • Update affected consoles and remove from Nessus Policy scan when deactivating a system <p>Interviewed the Manager of Security and IT Compliance and CISO & Senior Director of Reliability and determined the following:</p> <ul style="list-style-type: none"> • All production application assets are provided as Docker containers running under AWS ECS • Some application containers are based on Alpine Linux and others are based on Microsoft Windows • In all cases, however, AWS resources are configured using infrastructure-as-code practices based Terraform • AWS-based components, including ECS clusters, VPC networks, cloud firewalls, S3 buckets, and KMS are 	No Relevant Exceptions Noted

		<p>securely configured following industry best practices based on AWS and Center for Internet Security (CIS) guidance</p> <p>Observed the use of Terraform and verified that it is used to configure AWS infrastructure and services</p> <p>Observed Dockerfile hardening and verified that it is consistent with CIS Docker benchmark recommendations</p>	
CC8.1.2	System configurations are reviewed on a daily basis.	<p>Interviewed the Manager of Security and IT Compliance and determined that daily reviews are performed by the Security team to confirm that critical security configurations remain in place</p> <p>Observed the IT Daily Security Check Log (dated September 2023) and verified that configurations are checked and reviewed daily on the following critical items:</p> <ul style="list-style-type: none"> • Email system • Microsoft Defender • Datadog – SQL Injection & SMS dashboard • CloudGuard • Microsoft Purview • AWS Macie 	No Relevant Exceptions Noted
CC8.1.3	The organization maintains formally documented roles and responsibilities for personnel involved in maintaining system configuration standards.	<p>Reviewed the Information Security Policies and Procedures document (dated August 7, 2023) and verified that the following personnel are responsible for system configuration standards:</p> <ul style="list-style-type: none"> • CTO or designated officer is responsible for coordinating and overseeing PayByPhone wide compliance with policies and procedures • The Systems Group is dedicated to security planning, education, and awareness • Cloud Platform Infrastructure team manages the PayByPhone solutions production and development environments 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> Corporate IT Team is responsible for corporate user environments and services 	
CC8.1.4	<p>Change management policies and procedures are implemented and require the documentation of approval by authorized parties and the testing of functionality prior to implementation.</p>	<p>Reviewed the change management process within the Information Security Policies and Procedures (dated September 4, 2023) and verified the following:</p> <ul style="list-style-type: none"> All proposed changes to network devices, systems, and application configurations must follow this policy The party responsible for implementing the change is required to complete and submit the appropriate electronic change request to the Systems Group’s manager or the manager of the Research and Development team Changes must receive management approval by the CTO, designated officer, or manager assigning the task Changes must be tested on a QA or test network that is isolated from the production Test plan should be followed to ensure there are no adverse effects If any discrepancies between expected and actual results that impact the network, systems, applications, business requirements, or support procedures occur, the documented back out procedures are immediately implemented <p>Interviewed the Manager of Security and IT Compliance and CISO & Senior Director of Reliability and determined the following:</p> <ul style="list-style-type: none"> Change management practices are implemented to ensure that changes to the system are controlled All changes to both infrastructure and applications are managed through a single process that is implemented through Jira tickets 	<p>No Relevant Exceptions Noted</p>

		<ul style="list-style-type: none"> • Changes are tested in pre-production environments consisting of development, integration, and consolidation prior to implementation in production <p>Observed the use of Jira tickets for tracking all changes and verified that Jira tickets capture the following information:</p> <ul style="list-style-type: none"> • Links to related pull and merge requests where application code review results and other necessary application details are captured • A description of the change and associated risks • Necessary approvals prior to implementing the changes • Testing results, including both manual and CI-driven testing • Backout plans in the even the change is unsuccessful <p>Observed that all changes are implemented as infrastructure-as-code and verified that the change followed the standard deployment pipeline, including testing in pre-production environments</p>	
CC8.1.5	Code reviews are conducted prior to changes being implemented.	<p>Reviewed the Code Reviews document and verified that the code review process is documented on Confluence; code reviews are required for every single code change; and reviewers must acknowledge in the review that the reviewed code is free from security defects before the review can be passed</p> <p>Interviewed the Manager of Security and IT Compliance and determined the following:</p> <ul style="list-style-type: none"> • Code reviews are necessary to allow a change to be made in production • Code reviews are completed by an individual (one or more developers and occasionally QAs) who did not write the code, and their review comment must indicate that they 	No Relevant Exceptions Noted

		<p>did a PCI or security assessment of the change</p> <ul style="list-style-type: none"> • If an issue is found, then the original coder addresses the issue, puts it back through QA, and completes the code review process before it can be deployed to production • Once deployed, it is smoke tested and, if deemed necessary for the change, further security testing with security testing tools is used in production • OWASP guidelines are reviewed and complied with during code reviews <p>Observed Jira tickets and verified that each deployment in Jira has a linked team ticket that contains the actual deployment branch</p>	
CC8.1.6	The organization maintains software development checklists to ensure the security during application development.	<p>Reviewed the Production Readiness Checklist and the Design Review Checklist and verified that the following security, compliance, and privacy standards are addressed:</p> <ul style="list-style-type: none"> • Code deploys are automated and run from a server or platform, not from developer machines • Deploys are zero-downtime, ensuring the availability of the service • Automated rollback is possible within five minutes or less • Terraform is used for deploying infrastructure • One-time database changes are source-controlled, and database schema changes are automated for non-legacy databases • Security review is performed by PayByPhone’s Security team, including risk assessment and penetration testing • Code is internally reviewed for security with respect to the OWASP Top 10 vulnerabilities 	No Relevant Exceptions Noted

		<ul style="list-style-type: none"> • Third-party library versions used have no known vulnerabilities, and licensing compliance is checked • APIs accessed by consumer apps or the back office use appropriate authentication mechanisms • Service logging is in place, excluding personally identifiable information (PII) and sensitive data • PII is hashed or encrypted using approved mechanisms and not written to logs • GDPR “right to be forgotten” is supported, allowing the removal or anonymization of personal data <p>Interviewed the Manager of Security and IT Compliance and determined that project management methodologies like Scrum, Kanban, and Scrumban are used, and work progress is tracked in Jira</p> <p>Interviewed the Manager of Security and IT Compliance and CISO & Senior Director of Reliability and determined that pipeline automation through GitLab CI is used to reduce the opportunities for human error in managing changes; once approved for introduction in the various operating environments, GitLab CI performs the deployment and measures the results with pre-defined tests to ensure that common errors are caught and corrected prior to production deployments; OWASP and general security best practices are always taken into account and are tracked in the Crucible code reviews</p> <p>Observed Jira tickets and verified that each deployment in Jira has a linked team ticket that contains the actual deployment branch</p>	
--	--	--	--

Common Criteria for the Privacy Category			
Risk Mitigation			
Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	<p>Risk mitigation activities are identified based on the results of the annual risk assessment and are selected by executive management.</p>	<p>Reviewed the Information Security Policies and Procedures (dated July 2023) and verified that the Systems Group and ITOPS team does the following:</p> <ul style="list-style-type: none"> • Conducts an annual formal risk assessments to identify new threats and vulnerabilities • Perform risk assessments when significant changes occur in the environment • Informs the company about information security issues and vulnerabilities • Monitors and identifies new security vulnerabilities and assigns risk rankings to them • Uses reputable outside sources for vulnerability information • Subscribes to vendor and security-specific internet mailing lists for threat identification • Maintains updates and patches for operating systems and applications <p>Interviewed the Manager of Security and IT Compliance and determined that the Compliance team reviews all risks monthly</p> <p>Interviewed the Manager of Security and Compliance and determined the following:</p> <ul style="list-style-type: none"> • At least annually, the organization coordinates a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks • Security risk assessments are reported and are shared with the Board on a quarterly basis 	<p>No Relevant Exceptions Noted</p>

		Observed the risk register and verified that a risk assessment resulted from a formal risk analysis in Q2 2023	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	Due diligence is performed prior to the selection of new vendors or service providers.	<p>Interviewed the Manager of Security and IT Compliance and determined that PayByPhone’s vendor due diligence procedures consists of the following:</p> <ul style="list-style-type: none"> • PayByPhone engages with a vendor for proof of concept (POC) early in the process • During POC, PayByPhone acquires compliance documentation, such as ISO 27000, SOC 2, and PCI AOC • If the vendor cannot provide appropriate audit reports, PayByPhone engages in a vendor risk assessment; the process is ad-hoc and tailored to the individual vendor • Legal is engaged for a contract once the POC is successful <p>Observed Zscaler documentation and verified that Zscaler underwent a full review before being accepted as a vendor</p>	No Relevant Exceptions Noted
CC9.2.2	Vendors and service providers are required to review and sign a non-disclosure agreement (NDA) and contract prior to sharing information with the organization.	<p>Interviewed the Manager of Security and IT Compliance and determined that PayByPhone signs NDAs with vendors prior to sharing any confidential information</p> <p>Observed the PayByPhone NDA template and verified that it is a mutual NDA that binds each receiving party to hold confidential information as disclosed by the disclosing party, and the agreement requires that the receiving party protects the information with no less than “reasonable care” and consistent with the measures it would take to protect its own confidential information</p>	No Relevant Exceptions Noted

		Observed completed contracts and verified that contracts are established between PayByPhone and their subservice organizations, where the subservice organizations commit to providing data security controls relevant to the services they provide	
CC9.2.3	Audit reports are required to be collected from vendors annually to ensure their continued compliance.	<p>Interviewed the Manager of Security and IT Compliance and determined that the organization has a process to manage vendors; the organization annually reviews all critical vendors and gathers the most recent audit reports, such as ISO 27000, SOC 2, and PCI DSS; when reviewing the SOC 2 exceptions, reasonable controls, and the opinion are reviewed</p> <p>Observed that the organization obtained AOCs from AWS, Azure, and Google and verified that the reports were obtained to review the third parties' compliance standing</p> <p>Observed SOC review tickets and verified that SOC 2 reports are reviewed as part of the vendor monitoring process</p>	No Relevant Exceptions Noted











PayByPhone 2024 Contract (32400116)


Final Audit Report


2024-04-06


Created:	2024-04-03
By:	Franz Lumbad (FLumbad@kirklandwa.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAA5QqAkDb5Dp1ofOd-QAdvbPk3UINKHiR7


"PayByPhone 2024 Contract (32400116)" History


-  Document created by Franz Lumbad (FLumbad@kirklandwa.gov)
2024-04-03 - 10:30:18 PM GMT- IP address: 76.191.73.2
-  Document emailed to charles.riddle@paybyphone.com for signature
2024-04-03 - 10:34:28 PM GMT
-  Email viewed by charles.riddle@paybyphone.com
2024-04-03 - 10:51:10 PM GMT- IP address: 52.102.12.69
-  Document signing delegated to Teresa Trussell (ttrussell@paybyphone.com) by charles.riddle@paybyphone.com
2024-04-04 - 3:18:22 PM GMT- IP address: 174.6.104.222
-  Document emailed to Teresa Trussell (ttrussell@paybyphone.com) for signature
2024-04-04 - 3:18:23 PM GMT
-  Email viewed by Teresa Trussell (ttrussell@paybyphone.com)
2024-04-04 - 3:18:40 PM GMT- IP address: 104.47.75.190
-  Document e-signed by Teresa Trussell (ttrussell@paybyphone.com)
Signature Date: 2024-04-04 - 3:21:13 PM GMT - Time Source: server- IP address: 206.55.214.210
-  Document emailed to Leta Santangelo (LSantangelo@kirklandwa.gov) for delegation
2024-04-04 - 3:21:15 PM GMT
-  Document approval delegated to Stephanie Croll (scroll@kirklandwa.gov) by Leta Santangelo (LSantangelo@kirklandwa.gov)
2024-04-04 - 8:01:17 PM GMT- IP address: 76.191.73.2
-  Document emailed to Stephanie Croll (scroll@kirklandwa.gov) for approval
2024-04-04 - 8:01:17 PM GMT


 Document approved by Stephanie Croll (scroll@kirklandwa.gov)
Approval Date: 2024-04-04 - 10:06:04 PM GMT - Time Source: server- IP address: 76.191.73.2


 Document emailed to Mary Jensen (mjensen@kirklandwa.gov) for signature
2024-04-04 - 10:06:06 PM GMT

 Email viewed by Mary Jensen (mjensen@kirklandwa.gov)
2024-04-04 - 10:27:27 PM GMT- IP address: 76.191.73.2


 Document e-signed by Mary Jensen (mjensen@kirklandwa.gov)
Signature Date: 2024-04-04 - 10:27:57 PM GMT - Time Source: server- IP address: 76.191.73.2


 Document emailed to Julie Underwood (junderwood@kirklandwa.gov) for signature
2024-04-04 - 10:28:00 PM GMT


 Email viewed by Julie Underwood (junderwood@kirklandwa.gov)
2024-04-05 - 10:58:29 PM GMT- IP address: 76.191.73.2

 Document e-signed by Julie Underwood (junderwood@kirklandwa.gov)
Signature Date: 2024-04-05 - 10:59:10 PM GMT - Time Source: server- IP address: 76.191.73.2

 Document emailed to JamieLynn Estell (jestell@kirklandwa.gov) for delivery
2024-04-05 - 10:59:13 PM GMT

 Email viewed by JamieLynn Estell (jestell@kirklandwa.gov)
2024-04-06 - 0:57:48 AM GMT- IP address: 50.46.38.43

 Document receipt acknowledged by JamieLynn Estell (jestell@kirklandwa.gov)
Receipt Acknowledgement Date: 2024-04-06 - 0:57:56 AM GMT - Time Source: server- IP address: 50.46.38.43

 Agreement completed.
2024-04-06 - 0:57:56 AM GMT