



**AMERICAN EXPRESS**

# Data Security Requirements

## Canada

October 2020

This document is intended for use by Merchants that have entered into a legally binding agreement with a Canadian-based Merchant Services Provider to accept the American Express® Card.

*DON'T do business* WITHOUT IT™



As a leader in consumer protection, American Express has a long-standing commitment to protect Cardholder Data and Sensitive Authentication Data, ensuring that it is kept secure. Compromised data negatively impacts consumers, Merchants, Service Providers and card issuers. Even one incident can severely damage a company's reputation and impair its ability to effectively conduct business. Addressing this threat by implementing security operating policies can help improve customer trust, increase profitability, and enhance a company's reputation.

American Express knows that Merchants (you) share our concern and requires, as part of your responsibilities, that you comply with the data security provisions in your agreement with your Merchant Services Provider to accept the American Express® Card (the Agreement) and these Data Security Requirements, which we may amend from time to time. These requirements apply to all your equipment, systems, and networks (and their components) on which Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) are stored, processed, or transmitted.

Capitalized terms used but not defined herein have the meanings ascribed to them in the glossary at the end of this policy.

## Section 1 Standards for Protection of Encryption Keys, Cardholder Data, and Sensitive Authentication Data

You must, and you must cause your Covered Parties to:

- store Cardholder Data only to facilitate American Express Card Transactions in accordance with, and as required by, the Agreement;
- comply with the current PCI DSS and other PCI SSC Requirements applicable to your processing, storing, or transmitting of Cardholder Data or Sensitive Authentication Data no later than the effective date for implementing that version of the applicable PCI SSC Requirement; and
- use, when deploying new or replacement PIN Entry Devices or Payment Applications (or both), in attended locations only those that are PCI-Approved.

You must protect all American Express Charge records, and Credit records retained pursuant to the Agreement in accordance with these data security provisions; you must use these records only for purposes of the Agreement and safeguard them accordingly. You are financially and otherwise liable to American Express for ensuring your Covered Parties' compliance with these data security provisions (other than for demonstrating your Covered Parties' compliance with this policy under [Section 4](#) below).

## Section 2 Data Incident Management Obligations

You must notify your Merchant Services Provider immediately after discovery of a Data Incident. In addition:

- You must conduct a thorough forensic investigation of each Data Incident.
- For Data Incidents involving 10,000 or more unique Card Numbers, you must engage a PCI Forensic Investigator (**PFI**) to conduct this investigation within five (5) days following discovery of a Data Incident.
- The *unedited* forensic investigation report must be provided to your Merchant Services Provider in accordance with their time frame for providing such information.
- You must promptly provide to your Merchant Services Provider all Compromised Card Numbers. American Express reserves the right to conduct its own internal analysis to identify Card Numbers involved in the Data Incident.

Forensic investigation reports must be completed using the current Forensic Incident Final Report Template available from PCI. Such report must include forensic reviews, reports on compliance, and all other information related to the Data Incident; identify the cause of the Data Incident; confirm whether or not you were in compliance with the PCI DSS at the time of the Data Incident and verify your ability to prevent future Data Incidents (i) by providing a plan for remediating all PCI DSS deficiencies and (ii) participating in the American Express Compliance program (as described below). Upon your Merchant Services Provider's request, you shall provide validation by a Qualified Security Assessor (**QSA**) that the deficiencies have been remediated.

Notwithstanding the foregoing paragraphs of this [Section 2](#):

- American Express may, in its sole discretion, require you to engage a PFI to conduct an investigation of a Data Incident for Data Incidents involving less than 10,000 unique Card Numbers. Any such investigation must comply with the requirements set forth above in this [Section 2](#), and must be completed within the time frame required by American Express.
- American Express may, in its sole discretion, separately engage a PFI to conduct an investigation for any Data Incident and may charge the cost of such investigation to you.

You must work with your Merchant Services Provider and American Express to rectify any issues arising from the Data Incident, including consultations about your communications to Cardmembers affected by the Data Incident and providing (and obtaining any waivers necessary to provide) to your Merchant Services Provider all relevant information to verify your ability to prevent future Data Incidents in a manner consistent with the Agreement.

Notwithstanding any contrary confidentiality obligation in the Agreement, American Express has the right to disclose information about any Data Incident to American Express Cardmembers, Issuers, other participants on the American Express Network, and the general public as required by applicable law; by judicial, administrative, or regulatory order, decree, subpoena, request, or other process in order to mitigate the risk of fraud or other harm or otherwise to the extent appropriate to operate the American Express Network.

## Section 3 Reserved

## Section 4 IMPORTANT! Periodic Validation of Your Systems

You must take the following actions to validate under PCI DSS annually and quarterly as described below, the status of your equipment, systems and/or networks (and their components) on which Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) are stored, processed, or transmitted.

There are four actions required to complete validation:

**Action 1** – Participate in American Express' compliance program under this policy.

**Action 2** – Understand your Level and Validation Requirements.

**Action 3** – Complete the Validation Documentation that you must send to your Merchant Services Provider.

**Action 4** – Send the Validation Documentation to your Merchant Services Provider within the prescribed timelines.

### Action 1 Participate in American Express' Compliance Program under this Policy

Level 1 Merchants and Level 2 Merchants, as described below, must participate in American Express' PCI Compliance Program under this policy by providing the full name, email address, telephone number, and physical mailing address of an individual who will serve as their data security contact. You must submit this information to your Merchant Services Provider. You must notify your Merchant Services Provider if this information changes, providing updated information where applicable. Your failure to provide such contact information may result in the assessment of non-compliance fees. Please contact your Merchant Services Provider for more information regarding its data security compliance requirements.

American Express may designate, at our sole discretion, certain Level 3 and Level 4 Merchants participation in American Express' compliance program under this policy by sending them written notice. The Merchant must enrol in the compliance program no later than 90 days following receipt of the notice.

### Action 2 Understand your Level and Validation Requirements

Merchant levels are based on your volume of American Express Card Transactions. For Merchants, this is the volume submitted by their establishments. You will fall into one of the Levels specified below.

#### Merchant Requirements

Merchants have four (4) possible classifications regarding their level and validation requirements. After determining the Merchant level from the list below, see the Merchant Table to determine validation documentation requirements.

**Level 1 Merchant** – 2.5 million American Express Card Transactions or more per year; or any Merchant that American Express otherwise, in its discretion, assigns a Level 1.

**Level 2 Merchant** – 50,000 to 2.5 million American Express Card Transactions per year.

**Level 3 Merchant** – 10,000 to 50,000 American Express Card Transactions per year.

**Level 4 Merchant** – Less than 10,000 American Express Card Transactions per year.

Merchant Level/ Annual American Express Transactions	Validation Documentation		
	On-Site Assessment Report on Compliance (ROC)	Self Assessment Questionnaire (SAQ) and Quarterly Network Scan	STEP Attestation for eligible Merchants
Level 1/ 2.5 million or more	Mandatory	Not applicable	Optional (replaces ROC)
Level 2/ 50,000 to 2.5 million	Optional	SAQ mandatory (unless submitting an On-Site Assessment) scan mandatory with certain SAQ types	Optional (replaces SAQ and network scan or ROC)
Level 3*/ 10,000 to 50,000	Optional	SAQ optional (mandatory if required by American Express) scan mandatory with certain SAQ types	Optional (replaces SAQ and network scan or ROC)
Level 4*/ 10,000 or less	Optional	SAQ optional (mandatory if required by American Express) scan mandatory with certain SAQ types	Optional (replaces SAQ and network scan or ROC)

\* For the avoidance of doubt, Level 3 and Level 4 Merchants need not submit Validation Documentation, unless required in American Express' discretion, but nevertheless must comply with, and are subject to liability under all other provisions of these Data Security Requirements.

American Express reserves the right to verify the accuracy and appropriateness of the PCI validation documentation provided as needed, including by engaging, at American Express' expense, a QSA or PFI of our choice.

**Security Technology Enhancement Program (STEP)** – Merchants that are compliant with PCI DSS may also, at American Express' discretion, qualify for American Express' STEP if they deploy certain additional security technologies throughout their Card processing environments. STEP applies only if the merchant has not experienced a Data Incident in the previous twelve (12) months and if 75% of all merchant Card Transactions are performed using:

- **EMV Technology** – on an active Chip-Enabled Device having a valid and current EMVCo ([www.emvco.com](http://www.emvco.com)) approval/certification and capable of processing AEIPS compliant Chip Card Transactions.
- **Point-to-Point Encryption (P2PE)** – communicated to the Merchant's processor using a PCI-SSC-approved or QSA-approved Point-to-Point Encryption system.

Merchants eligible for STEP have reduced PCI Validation Documentation requirements, as further described in [Action 3](#) below.

### Action 3 Complete the Validation Documentation that you must send to your Merchant Services Provider

The following documents are required for different levels of Merchants as indicated in the Merchant Table above.

**Annual Onsite Security Assessment** – The Annual Onsite Security Assessment is a detailed onsite examination of your equipment, systems, and networks (and their components) where Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) are stored, processed, or transmitted. It must be performed by

- a QSA or

- you and attested by your chief executive officer, chief financial officer, chief information security officer, or principal and submitted annually to your Merchant Services Provider on the applicable Attestation of Compliance (AOC).

The AOC must support compliance with all requirements of the PCI DSS and, upon request, include copies of the full report on compliance (Level 1 Merchants).

**Annual Self Assessment Questionnaire** – The Annual Self Assessment is a process using the PCI DSS Self-Assessment Questionnaire (SAQ) that allows self-examination of your equipment, systems, and networks (and their components) where Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) are stored, processed, or transmitted. It must be performed by you and certified by your chief executive officer, chief financial officer, chief information security officer, or principal. The AOC section of the SAQ must be submitted annually to your Merchant Services Provider. The AOC section of the SAQ must certify your compliance with all requirements of the PCI DSS and include full copies of the SAQ on request (Level 2, Level 3, and Level 4 Merchants).

**Quarterly Network Scan** – The Quarterly Network Scan is a process that remotely tests your Internet-connected computer networks and web servers for potential weaknesses and vulnerabilities. It must be performed by an Approved Scanning Vendor (ASV). You must complete and submit the ASV Scan Report Attestation of Scan Compliance (AOSC) or the executive summary of findings of the scan (and copies of the full scan, on request) quarterly to your Merchant Services Provider. The AOSC or executive summary must certify that the results satisfy the PCI DSS scanning procedures, that no high risk issues are identified, and that the scan is passing or compliant (all Merchants except those who also submit an Onsite Security Assessment Report and STEP-eligible Merchants). For the avoidance of doubt, Quarterly Network Scans are mandatory if required by the applicable Self Assessment Questionnaire.

**Annual STEP Attestation Validation Documentation** – The American Express Annual STEP Attestation (STEP Attestation) is available only to merchants who meet the criteria listed in [Action 2](#) above. The STEP Attestation involves a process using PCI DSS requirements that allows self-examination of your equipment, systems, and networks (and their components) where Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) are stored, processed, or transmitted. It must be performed by you and certified by your chief executive officer, chief financial officer, chief information security officer, or principal. You must complete the process by submitting the STEP Attestation form annually to your Merchant Services Provider. (STEP-eligible Merchants only).

**Summary of Compliance** – The Summary of Compliance (SOC) is a document by which a Franchisor or Service Provider may report the PCI Compliance status of its franchisees. The SOC template is available for download via SecureTrust's secure portal.

**Non Compliance with PCI DSS** – If you are not compliant with the PCI DSS, then you must submit one of the following documents:

- an Attestation of Compliance (AOC) including "Part 4. Action Plan for Non-Compliant Status"
- a PCI Prioritized Approach Tool Summary and Attestation of Compliance (PASAOC)
- a Project Plan Template (available from your Merchant Services Provider)

Each of the above documents must designate a remediation date, not to exceed twelve (12) months following the document completion date in order to achieve compliance. You must submit the appropriate document to your Merchant Services Provider. You shall provide your Merchant Services Provider with periodic updates of your progress toward remediation of your Non-Compliant Status (Level 1, Level 2, Level 3, and Level 4 Merchants). For the avoidance of all doubt, Merchants that are not compliant with PCI DSS are not eligible for STEP.

## Action 4 Send the Validation Documentation to your Merchant Services Provider

All Merchants required to participate in the American Express PCI Compliance Program must submit the Validation Documentation marked "mandatory" in the table in [Action 2](#).

You must submit your Validation Documentation to your Merchant Services Provider. If you have general questions about the program or the process above, please contact your Merchant Services Provider.

Compliance and validation are completed at your expense. By submitting Validation Documentation to your Merchant Services Provider, you represent and warrant that you are authorized to disclose the information contained therein to your Merchant Services Provider and American Express, and are providing the Validation Documentation without violating any other party's rights.

### **Non-Validation Fees and Termination of Agreement**

American Express and your Merchant Services Provider have the right to impose non-validation fees on you and terminate the Agreement if you do not fulfil these requirements or fail to provide the mandatory Validation Documentation by the applicable deadline. Your Merchant Services Provider will notify you separately of the applicable deadline for each annual and quarterly reporting period.

If your Merchant Services Provider does not receive your mandatory Validation Documentation, then your Merchant Services Provider may have the right to terminate the Agreement in accordance with its terms as well as impose non-validation fees on you.

## **Section 5    Reserved**

## **Section 6    Disclaimer**

AMERICAN EXPRESS HEREBY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES, AND LIABILITIES WITH RESPECT TO THESE DATA SECURITY REQUIREMENTS, THE PCI DSS, THE EMV SPECIFICATIONS AND THE DESIGNATION AND PERFORMANCE OF QSAs, ASVs, OR PFIs (OR ANY OF THEM), WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AMERICAN EXPRESS CARD ISSUERS ARE NOT THIRD PARTY BENEFICIARIES UNDER THIS POLICY.

### **Useful Web Sites**

American Express Data Security Requirements:

[www.americanexpress.ca/dsr](http://www.americanexpress.ca/dsr)

PCI Security Standards Council, LLC:

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

## **Glossary of Terms**

For purposes of this policy only, the following definitions apply:

### **Account Status Check**

A type of Authorization request that is used to ask an Issuer to indicate if the Card account represented by the Card Number on the message is valid. The Account Status Check is used, for example, by transit authorities to check the status of a Card account associated with a Transit Contactless Transaction at transit operator's terminal.

### **American Express Card or Card**

Any card, account access device, or payment device or service bearing American Express' or an affiliate's name, logo, trademark, service mark, trade name, or other proprietary design or designation and issued by an issuer; or a card account number.

### **Approved Point-to-Point Encryption (P2PE) Solution**

Any solution included on PCI SSC list of validated solutions or validated by a PCI SSC Qualified Security Assessor P2PE Company.



**Approved Scanning Vendor or ASV**

An entity that has been qualified by the Payment Card Industry Security Standards Council, LLC to validate adherence to certain PCI DSS requirements by performing vulnerability scans of internet facing environments.

**Attestation of Compliance, or AOC**

A declaration of the status of your compliance with the PCI DSS, in the form provided by the Payment Card Industry Security Standards Council, LLC.

**Attestation of Scan Compliance, or AOSC**

A declaration of the status of your compliance with the PCI DSS based on a network scan, in the form provided by the Payment Card Industry Security Standards Council, LLC.

**Card Number**

The unique identifying number that the Issuer assigns to the Card when it is issued.

**Cardholder Data**

The meaning given to it in the then current Glossary of Terms for the PCI DSS.

**Cardmember**

An individual or entity (i) that has entered into an agreement establishing a Card account with an issuer or (ii) whose name appears on the Card.

**Charge**

A payment or purchase made on a Card.

**Chip**

An integrated microchip embedded on a Card containing Cardmember and account information.

**Chip Card**

A Card that contains a Chip and could require a PIN as a means of verifying the identity of the Cardmember or account information contained in the Chip, or both (sometimes called a "smart card", an "EMV Card", or an "ICC" or "integrated circuit card" in our materials).

**Chip-Enabled Device**

A point-of-sale device having a valid and current EMVCo ([www.emvco.com](http://www.emvco.com)) approval/certification and be capable of processing AEIPS compliant Chip Card Transactions.

**Compromised Card Number**

An American Express Card account number related to a Data Incident.

**Covered Parties**

Any or all of your employees, agents, representatives, subcontractors, Processors, Service Providers, providers of your point-of-sale (POS) equipment or systems or payment processing solutions, entities associated to your American Express merchant account, and any other party to whom you may provide Cardholder Data or Sensitive Authentication Data (or both) access in accordance with the Agreement.

**Credit**

The amount of the Charge that you refund to Cardmembers for purchases or payments made on the Card.



## Data Incident

An incident involving the compromise or suspected compromise of American Express Encryption Keys, or at least one American Express Card account number in which there is:

- unauthorized access or use of Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) that are stored, processed, or transmitted on your equipment, systems, and/or networks (or the components thereof) of yours or the use of which you mandate;
- use of such Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each) other than in accordance with the Agreement; and/or
- suspected or confirmed loss, theft, or misappropriation by any means of any media, materials, records, or information containing such Encryption Keys, Cardholder Data, or Sensitive Authentication Data (or a combination of each).

## Data Incident Event Window

The period that begins as of the date of compromise, if known, or 365 days prior to the Notification Date if the actual date of compromise is not known. The Data Incident Event Window ends 30 days after the Notification Date.

## EMV Specifications

The specifications issued by EMVCo, LLC, which are available at [www.emvco.com](http://www.emvco.com).

## EMV Transaction

An integrated circuit card (sometimes called an "IC Card," "chip card," "smart card," "EMV card," or "ICC") transaction conducted on an IC card capable point of sale (POS) terminal with a valid and current EMV type approval. EMV type approvals are available at [www.emvco.com](http://www.emvco.com).

## Encryption Key ("American Express encryption key")

All keys used in the processing, generation, loading and/or protection of account data. This includes, but is not limited to, the following:

- Key Encrypting Keys: Zone Master Keys (ZMKs) and Zone Pin Keys (ZPKs)
- Master Keys used in secure cryptographic devices: Local Master Keys (LMKs)
- Card Security Code Keys (CSCs)
- PIN Keys: Base Derivation Keys (BDKs), PIN Encryption Key (PEKs), and ZPKs

## Forensic Incident Final Report Template

The template available from the PCI Security Standards Council which is available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

## Franchisee

An independently owned and operated third party (including a franchisee, licensee, or chapter) other than an Affiliate that is licensed by a Franchisor to operate a franchise and that has entered into a written agreement with the Franchisor whereby it consistently displays external identification prominently identifying itself with the Franchisor's Marks or holds itself out to the public as a member of the Franchisor's group of companies.

## Franchisor

The operator of a business that licenses persons or Entities (Franchisees) to distribute goods and/or services under, or operate using the operator's mark; provides assistance to Franchisees in operating their business or influences the Franchisee's method of operation; and requires payment of a fee by Franchisees.

**Level 1 Merchant**

2.5 million American Express Card Transactions or more per year; or any Merchant or that American Express otherwise deems a Level 1.

**Level 2 Merchant**

50,000 to 2.5 million American Express Card Transactions per year.

**Level 3 Merchant**

10,000 to 50,000 American Express Card Transactions per year.

**Level 4 Merchant**

Less than 10,000 American Express Card Transactions per year.

**Merchant**

The merchant and all of its affiliates that have entered into a legally binding merchant agreement with a Merchant Services Provider based in Canada to accept the American Express® Card.

**Merchant Services Provider**

Merchant's payment card processor or any Entity with which Merchant receives merchant processing services. These services may include, but are not limited to, processing transactions, facilitating authorizations on purchases, and capturing data, merchant accounting, backroom operations (e.g., chargebacks and detecting fraud), provision of point of sale equipment, solutions, or systems, sales, or customer service.

**Notification Date**

The date that American Express provides issuers with final notification of a Data Incident. Such date is contingent upon American Express' receipt of the final forensic report or internal analysis and shall be determined in American Express' sole discretion.

**Payment Application**

Has the meaning given to it in the then-current Glossary of Terms for Payment Card Industry Payment Application Data Security Standard, which is available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Payment Card Industry Security Standards Council (PCI SSC) Requirements**

The set of standards and requirements related to securing and protecting payment card data, including the PCI DSS and PA DSS, available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**PCI-Approved**

A PIN Entry Device or a Payment Application (or both) appears at the time of deployment on the list of approved companies and providers maintained by the PCI Security Standards Council, LLC, which is available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**PCI DSS**

Payment Card Industry Data Security Standard, which is available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**PCI Forensic Investigator or PFI**

An entity that has been approved by the Payment Card Industry Security Standards Council, LLC to perform forensic investigations of a breach or compromise of payment card data.

**PCI PIN Security Requirements**

The Payment Card Industry PIN Security Requirements which is available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**PIN Entry Device**

Has the meaning given to it in the then-current Glossary of Terms for the Payment Card Industry PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements, which is available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Point of Sale (POS) System**

An information processing system or equipment, including a terminal, personal computer, electronic cash register, contactless reader, or payment engine or process, used by a Merchant, to obtain authorizations or to collect Transaction data, or both.

**Point-to-Point Encryption (P2PE)**

A solution that cryptographically protects account data from the point where a Merchant accepts the payment card to the secure point of decryption.

**Processor**

A service provider to Merchants who facilitate authorization and submission processing to the American Express Network.

**Qualified Security Assessor or QSA**

An entity that has been qualified by the Payment Card Industry Security Standards Council, LLC to validate adherence to the PCI DSS.

**Security Technology Enhancement Program (STEP)**

American Express' program in which Merchants are encouraged to deploy technologies that improve data security. To qualify for STEP, Merchants must not have had a Data Incident in the 12 months prior to submitting the Annual Attestation of Compliance and conducted at least 75% of all Transactions using Point-to-Point Encryption or face-to-face Transactions using EMV Chip Enabled Devices.

**Self-Assessment Questionnaire or SAQ**

A self assessment tool created by the Payment Card Industry Security Standards Council, LLC, intended to evaluate and attest to compliance with the PCI DSS.

**Sensitive Authentication Data**

Has the meaning given it in the then-current Glossary of Terms for the PCI DSS.

**Service Providers**

Authorized processors, third party processors, gateway providers, integrators of POS Systems, and any other providers to Merchants of POS Systems, or other payment processing solutions or services.

**Summary of Compliance or SOC**

A PCI validation document used by a Franchisor to indicate the PCI compliance status of its affected franchisees.

**Transaction**

A Charge or a Credit completed by means of a Card.

**Validation Documentation**

The AOC rendered in connection with an Annual Onsite Security Assessment or SAQ, the AOSC and executive summaries of findings rendered in connection with Quarterly Network Scans, or the annual STEP Attestation.