



# AMERICAN EXPRESS

# Data Security Requirements

## United States Region

October 2023

This document is intended for use by Merchants that have entered into a legally binding agreement with a U.S.-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 those) 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 Targeted Analysis Program (TAP)

Cardholder Data compromises may be caused by data security gaps in your Cardholder Data Environment (CDE). Examples of Cardholder Data compromise include, but are not limited to:

- **Common Point of Purchase (CPP):** American Express Cardmembers report fraudulent Transactions on their Card accounts and are identified and determined to have originated from making purchases at your Establishments.
- **Card Data found:** American Express Card and Cardholder Data found on the world wide web linked to Transactions made at your Establishments.
- **Malware suspected:** American Express suspects that your business is using software infected with or vulnerable to malicious code.

TAP is designed to identify potential Cardholder Data compromises.

You must, and you must cause your Covered Parties to, comply with the following requirements upon notification from American Express or your Merchant Services Provider, of a potential Cardholder Data compromise.

- You must promptly review your CDE for data security gaps and remediate any findings.
  - You must cause your third-party vendor(s) to conduct a thorough investigation of your CDE if outsourced.
- You must provide a summary of action taken or planned after your review, evaluation, and/or remediation efforts upon notification from American Express or your Merchant Services Provider.
- You must provide updated PCI DSS validation documents in accordance with [Section 5, "Periodic Validation of Merchant Systems"](#).
- As applicable, you must engage a qualified PCI Forensic Investigator (PFI) to examine your CDE if you or your Covered Party:
  - Cannot resolve the Cardholder Data compromise within a reasonable period of time, as determined by American Express, or
  - Confirm that a Data Incident has occurred and comply with the requirements set forth in [Section 3, "Data Incident Management Obligations"](#).

If you cannot meet these obligations, your Merchant Services Provider may have the right to terminate the Agreement in accordance with its terms as well as impose non-compliance fees on you.

## Section 2 Standards for Protection of Cardmember Information

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 requirement.
- use, when deploying new or replacement PIN Entry Devices or Payment Applications (or both), 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 5, "Periodic Validation of Merchant Systems"](#) except as otherwise provided in that section.)

## Section 3 Data Incident Management Obligations

You must notify your Merchant Services Provider immediately and in no case later than seventy-two (72) hours 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 by (i) 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 3, "Data Incident Management Obligations"](#):

- 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 3, "Data Incident Management Obligations"](#), 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 4 Reserved

## Section 5 Periodic Validation of Merchant Systems

You must take the following actions to validate under PCI DSS annually and quarterly as described below, the status of your and your Franchisees' equipment, systems, and/or networks (and their components) on which Cardholder Data or Sensitive Authentication Data 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 enroll in the compliance program no later than 90 days following receipt of the notice.

### Action 2 Understand your Merchant Level and Validation 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	Merchant Validation Documentation	
	Report on Compliance Attestation of Compliance (ROC AOC)	Questionnaire Attestation of Compliance (SAQ AOC and Quarterly External Network Vulnerability Scan (Scan))
Level 1/ 2.5 million or more	Mandatory	Not applicable
Level 2/ 50,000 to 2.5 million	Optional	SAQ AOC mandatory (unless submitting a ROC AOC); scan mandatory with certain SAQ types
Level 3*/ 10,000 to 50,000	Optional	SAQ AOC optional (mandatory if required by American Express); scan mandatory with certain SAQ types
Level 4*/ 10,000 or less	Optional	SAQ AOC optional (mandatory if required by American Express); scan mandatory with certain SAQ types

\* 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.

### Action 3 Complete the Validation Documentation

The following documents are required for different levels of Merchants as indicated in the Merchant Table above that you must send, if required, to your Merchant Services Provider.

You must provide the Attestation of Compliance (AOC) for the applicable assessment type. The AOC is a declaration of your compliance status and, as such, must be signed and dated by the appropriate level of leadership within your organization.

In addition to the AOC, American Express may require you to provide a copy of the full assessment and, at our discretion, additional supporting documents demonstrating compliance with the PCI DSS requirements. This Validation Documentation is completed at your expense.

**Report on Compliance Attestation of Compliance (ROC AOC) - (Annual Requirement)** – The Report on Compliance documents the results of a detailed onsite examination of your equipment, systems, and networks (and their components) where Cardholder Data or Sensitive Authentication Data (or both) are stored, processed, or transmitted. The Report on Compliance must be performed by:

- a QSA or
- you and attested by your chief executive officer, chief financial officer, chief information security officer, or principal.

The AOC must be signed and dated by a QSA or Internal Security Assessor (ISA) and the authorized level of leadership within your organization and provided to your Merchant Service Provider at least once per year.

**Self-Assessment Questionnaire Attestation of Compliance (SAQ AOC) - (Annual Requirement)** – The Self-Assessment Questionnaires allow self-examination of your equipment, systems, and networks (and their components) where Cardholder Data or Sensitive Authentication Data (or both) are stored, processed, or transmitted. There are multiple versions of the SAQ. You will select one or more based on your Cardholder Data Environment.

The SAQ may be completed by personnel within your Company qualified to answer the questions accurately and thoroughly or you may engage a QSA to assist. The AOC must be signed and dated by the authorized level of leadership within your organization and provided to your Merchant Service Provider at least once per year.

**Approved Scanning Vendor External Network Vulnerability Scan Summary (ASV Scan) - (90 Day Requirement)** – An external vulnerability scan is a remote test to help identify potential weaknesses, vulnerabilities, and misconfigurations of internet-facing components of your Cardholder Data Environment (e.g., websites, applications, web servers, mail servers, public-facing domains, or hosts).

The ASV Scan must be performed by an Approved Scanning Vendor (ASV).

If required by the SAQ, the ASV Scan Report Attestation of Scan Compliance (AOSC) or executive summary including a count of scanned targets, certification that the results satisfy PCI DSS scanning procedures, and compliance status completed by ASV, must be submitted to your Merchant Service Provider at least once every 90 days.

ROC or AOC are not required to provide an AOSC or ASV Scan executive summary unless specifically requested. For the avoidance of doubt, Scans are mandatory if required by the applicable SAQ.

**Non Compliance with PCI DSS - (Annual, 90 Day and/or Ad Hoc Requirement)** – 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" (available for download via the PCI Security Standards Council website)
- a PCI Prioritized Approach Tool Summary (available for download via the PCI Security Standards Council website)

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). Remediation actions necessary to achieve compliance with PCI DSS are to be completed at your expense.

## 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, Understand your Merchant Level and Validation Requirements](#).

You must submit your Validation Documentation to your Merchant Services Provider.

By submitting Validation Documentation, you represent and warrant to American Express that the following is true (to the best of your ability):

- Your evaluation was complete and thorough;
- The PCI DSS status is accurately represented at the time of completion, whether compliant or non-compliant;
- You are authorized to disclose the information contained therein and are providing the Validation Documentation to American Express 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 fulfill 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 6 Reserved

## Section 7 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.com/dsr](http://www.americanexpress.com/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:

### 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 (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 (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 (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.

### Cardholder Data

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

### Cardholder Data Environment (CDE)

The people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.

### 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.

### Card Number

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

### 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 with 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, or provide, or make available;
- 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 (a combination of each).

### Data Incident Event Window

The window of intrusion (or similarly determined period of time) set forth in the final forensic report (e.g., PFI report), or if unknown, up to 365 days prior to the last Notification Date of potentially Compromised Card Numbers involved in a Data Compromise reported to us.

### 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 (CSCKs)
- 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.

### Issuer

Any Entity (including American Express and its Affiliates) licensed by American Express or an American Express Affiliate to issue Cards and to engage in the Card issuing business.

### Level 1 Merchant

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

### Level 2 Merchant

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

### Level 3 Merchant

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

### Level 4 Merchant

A Merchant with 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 the United States Region 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 Secure Software Standard and Secure Software Life Cycle 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 (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 (QSA)

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

### Risk-Mitigating Technology

Technology solutions that improve the security of American Express Cardholder Data and Sensitive Authentication Data, as determined by American Express. To qualify as a Risk-Mitigating Technology, you must demonstrate effective utilization of the technology in accordance with its design and intended purpose. Examples include: EMV, Point-to-Point Encryption, and tokenization.

### Self-Assessment Questionnaire (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.

### Targeted Analysis Program

A program that provides early identification of a potential Cardholder Data compromise in your Cardholder Data Environment (CDE). See [Section 1, "Targeted Analysis Program \(TAP\)"](#).

### Transaction

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

### United States (U.S.) Region

Consists of the 50 United States and the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands, but no other U.S. territory or possession.

### 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 Security Technology Enhancement Program Attestation.