

Data Security Operating Policy (DSOP)

Change Bars

Important updates are listed in the Summary of Changes Table and also indicated in the *DSOP* with a change bar. A change bar alongside the title of a section or subsection denotes revised, added, or removed text from the section or subsection. Changes in the *DSOP* are indicated with a change bar as shown here:



Summary of Changes Table

Important updates are listed in the following table and are also indicated in the *DSOP* with a change bar.

Section/Subsection	Description of Change
There are no changes for this release.	

What to do if you have a Data Incident?

Please follow these steps if you have identified a Data Incident at your business.

**Step 1:**

Fill out the [Merchant Data Incident Initial Notice Form](#) and email to EIRP@aexp.com within 72 hours after the Data Incident is discovered.

**Step 2:**

Conduct a thorough investigation; this may require you to hire a [Payment Card Industry \(PCI\) Forensic Investigator](#).

**Step 3:**

Promptly provide us with all compromised American Express® Card numbers.

**Step 4:**

Work with us to help resolve any issues arising from the Data Incident.

View [Section 3 Data Incident Management Obligations](#) for more details on Data Incident Management Obligations.

Have more questions?

US: (888) 732-3750 (toll free)

International: +1 (602) 537-3021

EIRP@aexp.com

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 our Merchants and Service Providers (collectively, **you**) share our concern and requires, as part of your responsibilities, that you comply with the data security provisions in your agreement to accept (in the case of Merchants) or process (in the case of Service Providers) the American Express® Card (each, respectively, the **Agreement**) and this Data Security Operating Policy, 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 at your Establishments.
- **Malware Suspected:** American Express suspects you are 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, 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.
- You must provide updated PCI DSS validation documents in accordance with [Section 5. Important Periodic Validation of your 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](#).

Table 1: TAP Non-Compliance Fee

Description	Level 1 Merchant or Level 1 Service Provider	Level 2 Merchant or Level 2 Service Provider	Level 3 or Level 4 Merchant
Non-compliance fee may be assessed when TAP obligations are not satisfied by the first deadline.	USD \$25,000	USD \$5,000	USD \$1,000
Non-compliance fee may be assessed when TAP obligations are not satisfied by the second deadline.	USD \$35,000	USD \$10,000	USD \$2,500
Non-compliance fee may be assessed when TAP obligations are not satisfied by the third deadline. NOTE: <i>Non-compliance fees may continue to be applied until the obligations are met or TAP is resolved.</i>	USD \$45,000	USD \$15,000	USD \$5,000

If your TAP obligations are not satisfied, then American Express has the right to impose the Non-compliance fees cumulatively, withhold payments, and/or terminate the Agreement.

Section 2 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 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. Important Periodic Validation of your Systems](#), except as otherwise provided in that section).

Section 3 Data Incident Management Obligations

You must notify American Express immediately and in no case later than seventy-two (72) hours after discovery of a Data Incident.

To notify American Express, contact the American Express Enterprise Incident Response Program (EIRP) toll free at 1.888.732.3750, or at 1.602.537.3021, or email at EIRP@aexp.com. You must designate an individual as your contact regarding such 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 American Express within ten (10) business days of its completion.
- You must promptly provide to American Express 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 American Express' 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 timeframe 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 agree to work with American Express to rectify any issues arising from the Data Incident, including consulting with American Express about your communications to Cardmembers affected by the Data Incident and providing (and obtaining any waivers necessary to provide) to American Express 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 Indemnity Obligations for a Data Incident

Your indemnity obligations to American Express under the Agreement for Data Incidents shall be determined, without waiving any of American Express' other rights and remedies, under this [Section 4. Indemnity Obligations for a Data Incident](#). In addition to your indemnity obligations (if any), you may be subject to a Data Incident non-compliance fee as described below in this [Section 4. Indemnity Obligations for a Data Incident](#).

For Data Incidents that involve:

- 10,000 or more American Express Card Numbers with either of the following:
 - Sensitive Authentication Data, or
 - Expiration Date

you shall compensate American Express at the rate of \$5 USD per account number.

However, American Express will not seek indemnification from you for a Data Incident that involves:

- less than 10,000 American Express Card Numbers, or
- more than 10,000 American Express Card Numbers, if you meet the following conditions:
 - you notified American Express of the Data Incident pursuant to [Section 3. Data Incident Management Obligations](#),

- you were in compliance at the time of the Data Incident with the PCI DSS (as determined by the PFI’s investigation of the Data Incident), and
- the Data Incident was not caused by your wrongful conduct or that of your Covered Parties.

Notwithstanding the foregoing paragraphs of this [Section 4. Indemnity Obligations for a Data Incident](#), for any Data Incident, regardless of the number of American Express Card Numbers, you shall pay American Express a Data Incident non-compliance fee not to exceed \$100,000 USD per Data Incident (as determined by American Express in its sole discretion) in the event that you fail to comply with any of your obligations set forth in [Section 3. Data Incident Management Obligations](#). For the avoidance of doubt, the total Data Incident non-compliance fee assessed for any single Data Incident shall not exceed \$100,000 USD.

American Express will exclude from its calculation any American Express Card Account Number that was involved in a prior Data Incident indemnity claim made within the twelve (12) months prior to the Notification Date. All calculations made by American Express under this methodology are final.

American Express may bill you for the full amount of your indemnity obligations for Data Incidents or deduct the amount from American Express’ payments to you (or debit your Bank Account accordingly) pursuant to the Agreement.

Your indemnity obligations for Data Incidents hereunder shall not be considered incidental, indirect, speculative, consequential, special, punitive, or exemplary damages under the Agreement; provided that such obligations do not include damages related to or in the nature of lost profits or revenues, loss of goodwill, or loss of business opportunities.

In its sole discretion, American Express may reduce the indemnity obligation for Merchants solely for Data Incidents that meet each of the following criteria:

- Applicable Risk-Mitigating Technologies were used prior to the Data Incident and were in use during the entire Data Incident Event Window,
- A thorough investigation in accordance with the PFI program was completed (unless otherwise previously agreed in writing),
- Forensic report clearly states the Risk-Mitigating Technologies were used to process, store, and/or transmit the data at the time of the Data Incident, and
- You do not store (and did not store throughout the Data Incident Event Window) Sensitive Authentication Data or any Cardholder Data that has not been made unreadable.

Where an indemnity reduction is available, the reduction to your indemnity obligation (excluding any noncompliance fees payable), is determined as follows:

Table 2: Criteria for Indemnity Obligation Reduction

Indemnity Obligation Reduction	Required Criteria
Standard Reduction: 50%	>75% of total Transactions processed on Chip Enabled Devices ¹ OR Risk-Mitigating Technology in use at >75% of Merchant locations ²
Enhanced Reduction: 75% to 100%	>75% of all Transactions processed on Chip Enabled Devices ¹ AND another Risk-Mitigating Technology in use at >75% of Merchant locations ²

¹ As determined by American Express internal analysis

² As determined by PFI investigation

- The Enhanced Reduction (75% to 100%) shall be determined based on the lesser of the percentage of Transactions using Chip Enabled Devices AND Merchant locations using another Risk-Mitigating Technology. The examples below illustrate the calculation of the indemnity reduction.
- To qualify as using a Risk-Mitigating Technology, you must demonstrate effective utilization of the technology in accordance with its design and intended purpose. For example, deploying Chip Enabled Devices and processing Chip Cards as Magnetic Stripe or Key Entered Transactions, is NOT an effective use of this technology.
- The percentage of locations that use a Risk-Mitigating Technology is determined by PFI investigation.
- The reduction in the indemnity obligation does not apply to any non-compliance fees payable in relation to the Data Incident.

Table 3: Enhanced Indemnity Obligation Reduction

Ex.	Risk-Mitigating Technologies in use	Enhanced Indemnity Obligation Reduction Eligible?	Reduction
1	80% of Transactions on Chip Enabled Devices	No	50%: Standard Reduction (less than 75% use of Risk-Mitigating Technology does not qualify for Enhanced Reduction) ¹
	0% of locations use other Risk-Mitigating Technology		
2	80% of Transactions on Chip Enabled Devices	Yes	77%: Enhanced Reduction (based on 77% use of Risk-Mitigating Technology)
	77% of locations use other Risk-Mitigating Technology		
3	93% of Transactions on Chip Enabled Devices	Yes	93%: Enhanced Reduction (based on 93% of Transactions on Chip Enabled Devices)
	100% of locations use other Risk-Mitigating Technology		
4	40% of Transactions on Chip Enabled Devices	No	50%: Standard Reduction (less than 75% of Transactions on Chip Enabled Devices does not qualify for Enhanced Reduction)
	90% of locations use other Risk-Mitigating Technology		

¹ A Data Incident involving 10,000 American Express Card Accounts, at a rate of \$5 USD per account number (10,000 x \$5 = \$50,000 USD) may be eligible for a reduction of 50%, reducing the Indemnity Obligations from \$50,000 to \$25,000 USD, excluding any non-compliance fees.

Section 5 Important Periodic Validation of your Systems

You must take the following actions to validate under PCI DSS annually and every 90 days 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' PCI compliance program ("the Program") under this policy.

Action 2: Understand your Merchant Level and Validation Requirements.

Action 3: Complete the Validation Documentation that you must send to American Express.

Action 4: Send the Validation Documentation to American Express within the prescribed timelines.

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

Level 1 Merchants, Level 2 Merchants, and all Service Providers, as described below, must participate in the Program under this policy. American Express may designate, at our sole discretion, specific Level 3 and Level 4 Merchants to participate in the Program under this policy.

Merchants and Service Providers required to participate in the Program must enroll in the Portal provided by the Program Administrator selected by American Express within the prescribed timelines.

- You must accept all reasonable terms and conditions associated with the use of the Portal.
- You must assign and provide accurate information for at least one data security contact within the Portal. Required data elements include:
 - full name
 - email address
 - telephone number
 - physical mailing address
- You must provide updated or new contact information for the assigned data security contact within the Portal when the information changes.
- You must ensure your systems are updated to allow service communications from the Portal's designated domain.

Your failure to provide or maintain current data security contact information or enable email communications will not affect our rights to assess fees.

Action 2: Understand your Merchant Level and Validation Requirements

There are four Merchant Levels applicable to Merchants and two Levels applicable to Service Providers based on your volume of American Express Card Transactions.

- For Merchants, this is the volume submitted by their Establishments that roll up to the highest American Express Merchant account level.*
- For Service Providers, this is the sum of volume submitted by the Service Provider and Entities Service Provider to whom you provide services.

Buyer Initiated Payments (BIP) Transactions are not included in the volume of American Express Card Transactions to determine Merchant Level and validation requirements. You will fall into one of the Merchant Levels specified in the Merchant and Service Provider tables below.

*In the case of Franchisors, this includes volume from their Franchisee Establishments. Franchisors who mandate that their Franchisees use a specified Point of Sale (POS) System or Service Provider also must provide validation documentation for the affected Franchisees.

Merchant Validation Documentation Requirements

Merchants (not Service Providers) have four possible Merchant Level classifications. After determining the Merchant level from the list below, see [Table 4: Merchant Validation Documentation](#) 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.

Table 4: Merchant Validation Documentation

	Validation Documentation		
Merchant Level/ Annual American Express Transactions	Report on Compliance Attestation of Compliance (ROC AOC)	Questionnaire Attestation of Compliance (SAQ AOC) AND Quarterly External Network Vulnerability Scan (Scan)	STEP Attestation for eligible Merchants
Level 1/ 2.5 million or more	Mandatory	Not applicable	Optional with approval from American Express (replaces ROC)
Level 2/ 50,000 to 2.5 million	Optional	SAQ AOC mandatory (unless submitting a ROC AOC); scan mandatory with certain SAQ types	Optional (replaces SAQ and network scan or ROC)
Level 3*/ 10,000 to 50,000	Optional	SAQ AOC 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 AOC 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 this Data Security Operating Policy.

American Express reserves the right to verify the completeness, accuracy, and appropriateness of your PCI Validation Documentation. American Express may require you to provide additional supporting documents for evaluation in support of this purpose. Additionally, American Express has the right to require you to engage a PCI Security Standards Council approved QSA or PFI.

Security Technology Enhancement Program (STEP)

Merchants that are compliant with PCI DSS may, 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 12 months and if 75% of all Merchant Card Transactions are performed using a combination of the following enhanced security options:

- **EMV, EMV Contactless or Digital Wallet** – on an active Chip-Enabled Device having a valid and current EMVCo (www.emvco.com) approval/certification and capable of processing AEIPS compliant Chip Card Transactions. (U.S. Merchants must include Contactless)
- **Point-to-Point Encryption (P2PE)** – communicated to the Merchant's processor using a PCI-SSC-approved or QSA-approved Point-to-Point Encryption system
- **Tokenized** – the implemented tokenization solution must:
 - meet EMVCo specifications,
 - be secured, processed, stored, transmitted, and wholly managed by a PCI compliant third-party service provider, and
 - the Token cannot be reversed to reveal unmasked Primary Account Numbers (PANs) to the Merchant.

Merchants eligible for STEP have reduced PCI Validation Documentation requirements, as further described in [Action 3: Complete the Validation Documentation that you must send to American Express](#) below.

Service Provider Requirements

Service Providers (not Merchants) have two possible Level classifications. After determining the Service Provider Level from the list below, see [Table 5:Service Provider Documentation](#) to determine validation documentation requirements.

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

Level 2 Service Provider– less than 2.5 million American Express Card Transactions per year; or any Service Provider not deemed Level 1 by American Express.

Service Providers are not eligible for STEP.

Table 5: Service Provider Documentation

Level	Validation Documentation	Requirement
1	Annual Report on Compliance Attestation of Compliance (ROC AOC)	Mandatory
2	Annual SAQ D (Service Provider) and Quarterly Network Scan or Annual Report on Compliance Attestation of Compliance (ROC AOC), if preferred	Mandatory

It is recommended that Service Providers also comply with the PCI Designated Entities Supplemental Validation.

[Action 3: Complete the Validation Documentation that you must send to American Express](#)

The following documents are required for different levels of Merchants and Service Providers as listed in the [Table 4:Merchant Validation Documentation](#) and [Table 5:Service Provider Documentation](#) above.

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. There are two versions: one for Merchants and another for Service Providers. The Report on Compliance must be performed by:

- a QSA, or
- you and attested to 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 American Express 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 American Express 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 American Express at least once every 90 days.

ROC AOC or STEP 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.

STEP Attestation Validation Documentation (STEP) - (Annual Requirement) – STEP is only available to Merchants who meet the criteria listed in [Action 2: Understand your Merchant Level and Validation Requirements](#) above. If your company qualifies you must complete and submit the STEP Attestation form annually to American Express. The Annual STEP Attestation form is available to download from the Portal.

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)
- a Project Plan Template (available for download from the Portal). A Project Plan can be submitted in lieu of the annual attestation (SAQ/ROC) and/or in lieu of the scan requirement.

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 shall provide American Express with periodic updates of your progress toward remediation of your Non-Compliant Status (Level 1, Level 2, Level 3, and Level 4 Merchants; All Service Providers). Remediation actions necessary to achieve compliance with PCI DSS are to be completed at your expense.

American Express shall not impose non-validation fees (described below) on you for non-compliance prior to the remediation date, but you remain liable to American Express for all indemnity obligations for a Data Incident and are subject to all other provisions of this policy.

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 American Express](#)

All Merchants and Service Providers required to participate in the Program must submit the Validation Documentation marked “mandatory” in the tables in [Action 2: Understand your Merchant Level and Validation Requirements](#) to American Express by the applicable deadlines.

You must submit your Validation Documentation to American Express using the Portal provided by the Program Administrator selected by American Express. 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 has 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 to American Express by the applicable deadline. American Express will attempt to notify the data security contact of the applicable deadline for each annual and quarterly reporting period.

Table 6: Non-Validation Fee

Description	Level 1 Merchant or Level 1 Service Provider	Level 2 Merchant or Level 2 Service Provider	Level 3 or Level 4 Merchant
A non-validation fee will be assessed if the Validation Documentation is not received by the first deadline.	USD \$25,000	USD \$5,000	USD \$50
An additional non-validation fee will be assessed if the Validation Documentation is not received by the second deadline.	USD \$35,000	USD \$10,000	USD \$100
An additional non-validation fee will be assessed if the Validation Documentation is not received by the third deadline. NOTE: Non-validation fees will continue to be applied until the Validation Documentation is submitted.	USD \$45,000	USD \$15,000	USD \$250

If your PCI DSS Validation Documentation obligations are not satisfied, then American Express has the right to impose the non-validation fees cumulatively, withhold payments, and/or terminate the Agreement.

Section 6 Confidentiality

American Express shall take reasonable measures to keep (and cause its agents and subcontractors, including the Portal provider, to keep) your reports on compliance, including the Validation Documentation in confidence and not disclose the Validation Documentation to any third party (other than American Express' Affiliates, agents, representatives, Service Providers, and subcontractors) for a period of three years from the date of receipt, except that this confidentiality obligation does not apply to Validation Documentation that:

- a. is already known to American Express prior to disclosure;
- b. is or becomes available to the public through no breach of this paragraph by American Express;
- c. is rightfully received from a third party by American Express without a duty of confidentiality;
- d. is independently developed by American Express; or
- e. is required to be disclosed by an order of a court, administrative agency or governmental authority, or by any law, rule or regulation, or by subpoena, discovery request, summons, or other administrative or legal process, or by any formal or informal inquiry or investigation by any government agency or authority (including any regulator, inspector, examiner, or law enforcement agency).

Section 7 Disclaimer

AMERICAN EXPRESS HEREBY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES, AND LIABILITIES WITH RESPECT TO THIS DATA SECURITY OPERATING POLICY, 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 Websites

American Express Data Security: www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

Glossary

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

American Express Card, or Card, means 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, included on PCI SSC list of validated solutions or validated by a PCI SSC Qualified Security Assessor P2PE Company.

Approved Scanning Vendor (ASV) means 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) means 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) means 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.

Buyer Initiated Payment (BIP) means a payment Transaction enabled via a payment instruction file processed through BIP.

Cardholder Data has the meaning given to it in the then current Glossary of Terms for the PCI DSS.

Cardholder Data Environment (CDE) means the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.

Cardmember means 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.

Cardmember Information means information about American Express Cardmembers and Card Transactions, including names, addresses, card account numbers, and card identification numbers (CIDs).

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

Charge means a payment or purchase made on a Card.

Chip means an integrated microchip embedded on a Card containing Cardmember and account information.

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

Compromised Card Number means an American Express Card account number related to a Data Incident.

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

Data Incident means 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, 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 means 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 means the specifications issued by EMVCo, LLC, which are available at www.emvco.com.

EMV Transaction means 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.

Encryption Key (American Express encryption key) means 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, means the template available from the PCI Security Standards Council which is available at www.pcisecuritystandards.org.

Franchisee means 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 means 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 means 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 means 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 means a Merchant with 50,000 to 2.5 million American Express Card Transactions per year.

Level 3 Merchant means a Merchant with 10,000 to 50,000 American Express Card Transactions per year.

Level 4 Merchant means a Merchant with less than 10,000 American Express Card Transactions per year.

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

Level 2 Service Provider means a Service Provider with less than 2.5 million American Express Card Transactions per year; or any Service Provider not deemed Level 1 by American Express.

Merchant means the Merchant and all of its affiliates that accept American Express Cards under an Agreement with American Express or its affiliates.

Merchant Level means the designation we assign Merchants related to their PCI DSS compliance validation obligations, as described in Section 5 Important Periodic Validation of your Systems.

Notification Date means 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.

Payment Card Industry Data Security Standard (PCI DSS) means the Payment Card Industry Data Security Standard, which is available at <https://www.pcisecuritystandards.org>.

Payment Card Industry Security Standards Council (PCI SSC) Requirements means 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.

PCI-Approved means that 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.

PCI DSS means Payment Card Industry Data Security Standard, which is available at www.pcisecuritystandards.org.

PCI Forensic Investigator (PFI) means 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 means the Payment Card Industry PIN Security Requirements which is available at 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.

Point of Sale (POS) System means 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) means a solution that cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption.

Portal, The means the reporting system provided by the American Express PCI Program administrator selected by American Express. Merchants and Service Providers are required to use The Portal to submit PCI validation documentation to American Express.

Primary Account Number (PAN) has the meaning given to it in the then current Glossary of Terms for the PCI DSS.

Processor means a service provider to Merchants who facilitate authorization and submission processing to the American Express network.

Program, The means the American Express PCI Compliance Program.

Qualified Security Assessor (QSA) means 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 means 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 but may not be limited to: EMV, Point-to-Point Encryption, and tokenization.

Security Technology Enhancement Program (STEP) means the American Express' program in which Merchants are encouraged to deploy technologies that improve data security.

Self-Assessment Questionnaire (SAQ) means 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 means 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 (TAP) means a program that provides early identification of a potential Cardholder data compromise in your CDE. [See Section 1 – Targeted Analysis Program \(TAP\).](#)

Token means the cryptographic token that replaces the PAN, based on a given index for an unpredictable value.

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

Validation Documentation means 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.