



# Data Security Operating Policy (DSOP)

Section 1	Introduction to DSOP and Standards for Protection .....	3
Section 2	PCI DSS Compliance Program (Important Periodic Validation of your Systems) .....	3
Action 1:	Participate in American Express' Compliance Programme under this Policy.....	4
Action 2:	Understand your Merchant/Service Provider Level and Validation Documentation Requirements .....	4
Action 3:	Complete the Validation Documentation that you must send to American Express.....	7
Action 4:	Send the Validation Documentation to American Express .....	9
Section 3	Data Incident Management Obligations .....	10
Section 4	Indemnity Obligations for a Data Incident .....	12
Section 5	Targeted Analysis Programme (TAP) .....	14
Section 6	Confidentiality .....	15
Section 7	Disclaimer .....	15
Section 8	Glossary .....	16
Section 9	Useful Websites .....	19

# DSOP Summary of Changes

## Icons

 Important updates are listed in the Summary of Changes Table and also indicated in the *DSOP* with a change bar. A change bar is a vertical line, usually in the left margin, that identifies added or revised text. Only substantial changes in the *DSOP* with potential impacts to a Merchant’s operational procedures are indicated with a change bar as shown in the left margin.

 Removed text is highlighted with a trash can icon placed in the margin next to any significant deletion of text, including sections, tables, paragraphs, notes, and bullet points. Removed text is referenced in this Summary of Changes using the section numbering from the previous publication to avoid confusion.

---

Blue lines bordering paragraphs indicate region-specific information.

---

## 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.	

## Section 1 Introduction to DSOP and Standards for Protection

**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 (DSOP), 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.

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

The Data Security Operating Policy (DSOP) is a set of comprehensive policy requirements designed to protect Account Data whenever such data is stored, processed, or transmitted.

American Express requires all Merchants and Service Providers to be Payment Card Industry Data Security Standard (PCI DSS) compliant. As part of that requirement, 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 Security Standards Council (PCI-SSC) Requirements applicable to your processing, storing, or transmitting of Encryption Keys, Cardholder Data, or Sensitive Authentication Data, no later than the effective date for implementing that version of the applicable requirement.
- Ensure PCI-approved products are used when deploying or replacing technology to store, process, or transmit data.

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 2, "PCI DSS Compliance Program \(Important Periodic Validation of your Systems\)"](#), except as otherwise provided in that section). Details regarding the PCI standards and how to comply with their requirements can be found at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

## Section 2 PCI DSS Compliance Program (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 programme under this policy.
- [Action 2](#): Understand your Merchant/Service Provider Level and Validation Documentation 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 Programme under this Policy

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

Merchant and Service Providers required to participate in the Programme must enrol in the [Portal](#) provided by the Programme 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. The required information includes:
  - 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/Service Provider Level and Validation Documentation 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 [Table A-1: Merchant and Service Provider Levels](#).

\* 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.

Table A-1: Merchant and Service Provider Levels

Merchant Provider Level	Annual American Express Transactions
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 fewer than 2.5 million American Express Card Transactions per year.
Level 3 Merchant	10,000 to fewer than 50,000 American Express Card Transactions per year.
Level 4 Merchant	Fewer than 10,000 American Express Card Transactions per year.
Service Provider Level	Annual American Express Transactions
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	fewer than 2.5 million American Express Card Transactions per year; or any Service Provider not deemed Level 1 by American Express.

## Merchant Validation Documentation Requirements

Merchants (not Service Providers) have four possible Merchant Level classifications. After determining the Merchant level from [Table A-1: Merchant and Service Provider Levels](#) (above), see the [Table A-2: Merchant Validation Documentation](#) to determine validation documentation requirements.

**Table A-2: Merchant Validation Documentation**

Merchant Level/ Annual American Express Transactions	Report on Compliance Attestation of Compliance (ROC AOC)	Self-Assessment Questionnaire Attestation of Compliance (SAQ AOC) AND Quarterly External Network Vulnerability Scan (Scan)	Security Technology Enhancement Program (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 fewer than 2.5 million	Optional	SAQ AOC mandatory (unless submitting a ROC AOC); scan mandatory with certain SAQ types	Optional with approval from American Express* (replaces SAQ and network scan or ROC)
Level 3**/ 10,000 to fewer than 50,000	Optional	SAQ AOC optional (mandatory if required by American Express); scan mandatory with certain SAQ types	Optional with approval from American Express* (replaces SAQ and network scan or ROC)
Level 4**/ Fewer than 10,000	Optional	SAQ AOC optional (mandatory if required by American Express); scan mandatory with certain SAQ types	Optional with approval from American Express* (replaces SAQ and network scan or ROC)

\* **Note:** American Express PCI Team will review the request and eligibility and confirm if you qualify for the STEP Program. Please reach out to your Client Manager and/or [AXPPCIComplianceProgram@aexp.com](mailto:AXPPCIComplianceProgram@aexp.com) to check eligibility.

\*\*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 Qualified Security Assessor (QSA) or PCI Forensic Investigator (PFI).

## Service Provider Validation Documentation Requirements

Service Providers (not Merchants) have two possible Level classifications. After determining the Service Provider Level from [Table A-1: Merchant and Service Provider Levels](#) (above), see [Table A-3: Service Provider Validation Documentation](#) to determine validation documentation requirements.

Service Providers are not eligible for STEP.

**Table A-3: Service Provider Validation 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.

## Security Technology Enhancement Programme (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](http://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
- **Tokenised** – the implemented tokenisation 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.

## 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 [Table A-2: Merchant Validation Documentation](#) and [Table A-3: Service Provider Validation 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 organisation.

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
- an Internal security assessor (ISA) and attested to by your chief executive officer, chief financial officer, chief information security officer, or principal

The ROC AOC must be signed and dated by a QSA or ISA and the authorised level of leadership within your organisation 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 SAQ AOC must be signed and dated by the authorised level of leadership within your organisation 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.

If submitting a ROC AOC or STEP, you 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/Service Provider Level and Validation Documentation 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](#). You may also reach out to your Client Manager or write to American Express at [AXPPCIComplianceProgram@aexp.com](mailto:AXPPCIComplianceProgram@aexp.com).

**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 a PCI Prioritised Approach Tool (PAT) Summary (available for download via the PCI Security Standards Council website).

The PAT Summary 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 will not impose non-compliance fees prior to the remediation date. Per [Table A-4: Non-Compliance Fee](#), you remain liable to American Express for all indemnity obligations for a Data Incident and are subject to all other provisions of this policy.

American Express, at its sole discretion, retains the right to impose non-compliance fees if:

- a PCI Prioritised Approach Template has not been submitted in accordance with the requirements stated in this section,
- the remediation steps outlined in the PCI Prioritised Approach Template for Non-Compliant Status were not met,

- any of the requirements of the PCI Prioritised Approach Template for Non-Compliant Status were not fulfilled, or
- the mandatory compliance documentation was not provided to American Express by the applicable deadline or upon request.

Merchants/Service Providers that do not comply with the requirements detailed in [Action 2: Understand your Merchant/Service Provider Level and Validation Documentation Requirements](#), may be subject to fees as stated in [Action 4: Send the Validation Documentation to American Express](#).

**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 Programme must submit the Validation Documentation marked "mandatory" in the tables in [Action 2: "Understand your Merchant/Service Provider Level and Validation Documentation Requirements"](#) to American Express by the applicable deadlines.

You must submit your Validation Documentation to American Express using the [Portal](#) provided by the Programme 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 submitting the Attestation of Compliance (AOC) or a PCI Prioritised Approach Tool (PAT) Summary for non-compliance;
- You are authorised to disclose the information contained therein and are providing the Validation Documentation to American Express without violating any other party's rights.

## Non-Compliance Fees and Termination of Agreement

American Express has the right to impose non-compliance fees on you and terminate the Agreement if you do not fulfil 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 A-4: 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
A non-compliance 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-compliance 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-compliance fee will be assessed if the validation documentation is not received by the third deadline. <b>NOTE:</b> Non-compliance fees will continue to be applied until the validation documentation is submitted.	USD \$45,000	USD \$15,000	USD \$250

\* Non-Compliance Fees will be assessed in Local Currency equivalents.

\* Not applicable in Argentina.

If your PCI DSS compliance documentation 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 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 Programme (*EIRP*) toll free at 1.888.732.3750, or at 1.602.537.3021, or email at [EIRP@aexp.com](mailto:EIRP@aexp.com). You must designate an individual as your contact regarding such Data Incident. In addition:

- You must conduct a thorough investigation of each Data Incident and promptly provide to American Express all Compromised Card Numbers. American Express reserves the right to conduct its own internal analysis to identify data involved in the Data Incident.

For Data Incidents involving fewer than 10,000 unique Card Numbers, an investigation summary must be provided to American Express within ten (10) business days of its completion.

- Investigation summaries should contain the following information: incident summary, description of the affected environment(s), timeline of events, key dates, impact and data exposure details, containment and remediation actions, and attestation there is no indication additional American Express data is at-risk.

For Data Incidents involving 10,000 or more unique Card Numbers, you must engage a PCI 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.
- 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 fewer than 10,000 unique Card Numbers or where multiple incidents have occurred within a 12-month period. 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 must assess the Data Incident under applicable data breach notification laws globally and, where deemed necessary, notify applicable regulators and impacted Cardmembers in accordance with such data breach notification laws. If you have determined that your Service Provider or another entity is responsible for reporting the Data Incident, you shall advise such Service Provider or entity of its duty to assess its reporting obligations under applicable data breach notification laws. You agree to obtain written approval from American Express prior to referencing or naming American Express in any communications to Cardmembers about the Data Incident. You agree to work with American Express to provide details and rectify any issues arising from the Data Incident, including 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.

## 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](mailto: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](mailto:EIRP@aexp.com)

## 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"](#).

You shall compensate American Express at the rate of \$5 USD per account number, for Data Incidents that involve:

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

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

- fewer 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 USD \$100,000 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 USD \$100,000.

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 programme 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 non-compliance fees payable), is determined as follows:

**Table A-5: Criteria for Indemnity Obligation Reduction**

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

<sup>1</sup> As determined by American Express internal analysis

<sup>2</sup> 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 in [Table A-6: Enhanced Indemnity Obligation Reduction](#) illustrate the calculation of the indemnity reduction.
- To qualify as using a Risk-Mitigating Technology, you must demonstrate effective utilisation of the technology in accordance with its design and intended purpose.
- 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 A-6: Enhanced Indemnity Obligation Reduction

Ex.	Risk- Mitigating Technologies in use	Eligible	Reduction
1	<ul style="list-style-type: none"> <li>80% of Transactions on Chip Enabled Devices</li> <li>0% of locations use other Risk-Mitigating Technology</li> </ul>	No	50%: Standard Reduction (less than 75% use of Risk-Mitigating Technology does not qualify for Enhanced Reduction) <sup>1</sup>
2	<ul style="list-style-type: none"> <li>80% of Transactions on Chip Enabled Devices</li> <li>77% of locations use other Risk-Mitigating Technology</li> </ul>	Yes	77%: Enhanced Reduction (based on 77% use of Risk-Mitigating Technology)
3	<ul style="list-style-type: none"> <li>93% of Transactions on Chip Enabled Devices</li> <li>100% of locations use other Risk-Mitigating Technology</li> </ul>	Yes	93%: Enhanced Reduction (based on 93% of Transactions on Chip Enabled Devices)
4	<ul style="list-style-type: none"> <li>40% of Transactions on Chip Enabled Devices</li> <li>90% of locations use other Risk-Mitigating Technology</li> </ul>	No	50%: Standard Reduction (less than 75% of Transactions on Chip Enabled Devices does not qualify for Enhanced Reduction)

<sup>1</sup> A Data Incident involving 10,000 American Express Card Accounts, at a rate of USD \$5.00 per account number (10,000 x \$5 = USD \$50,000) may be eligible for a reduction of 50%, reducing the Indemnity Obligations from USD \$50,000 to USD \$25,000, excluding any non-compliance fees.

## Section 5 Targeted Analysis Programme (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 2, "PCI DSS Compliance Program \(Important Periodic Validation of your Systems\)"](#).
- As applicable, you must engage a qualified PCI 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 A-7: 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. <b>NOTE:</b> <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 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:

- is already known to American Express prior to disclosure;
- is or becomes available to the public through no breach of this paragraph by American Express;
- is rightfully received from a third party by American Express without a duty of confidentiality;
- is independently developed by American Express; or
- 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.

## Section 8 Glossary

For purposes of this *Data Security Operating Policy* only, the following definitions apply and control:

**Account Data** consists of Cardholder Data and/or sensitive authentication data. See Cardholder Data and Sensitive Authentication Data.

**Agreement** means the General Provisions, the Merchant Regulations, and any accompanying schedules and exhibits, collectively (sometimes referred to as the Card Acceptance Agreement in our materials).

**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) Transactions** means a digital payment solution that lets buyers quickly and efficiently schedule payments to suppliers (linked to corporate cards).

**Cardholder** means a customer to which payment card is issued, or any individual authorised to use the payment card.

**Cardholder Data** means at a minimum, the full Primary Account Number (PAN) by itself or full PAN plus any of the following: cardholder name, expiration date, and/or service code. See Sensitive Authentication Data for additional data elements that might be transmitted or processed (but not stored) as part of a payment transaction.

**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 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.

**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.

**Charge Record** means a reproducible (both paper and electronic) record of a Charge that complies with our requirements and contains the Card Number, Transaction date, dollar amount, Approval, Cardmember signature (if applicable), and other information.

**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](http://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.

**Consumer** is defined as a cardholder purchasing goods, services, or both.

**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.

**Credit Record** means a record of Credit that complies with our requirements.

**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:

- unauthorised 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** 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](http://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](http://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](http://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.

**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 fewer than 2.5 million American Express Card Transactions per year.

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

**Level 4 Merchant** means a Merchant with fewer 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 fewer 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 2, "PCI DSS Compliance Program \(Important Periodic Validation of your Systems\)"](#).

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

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

**PCI DSS** means Payment Card Industry Data Security Standard, which is available at [www.pcisecuritystandards.org](http://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](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** 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 authorisations 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 Programme 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 authorisation and submission processing to the American Express network.

**Programme, The** means the American Express PCI Compliance Programme.

**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 utilisation 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 tokenisation.

**Security Technology Enhancement Programme (STEP)** means the American Express programme 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** means security-related information used to authenticate cardholders and/or authorise payment card transactions. This information includes, but is not limited to, card verification codes, full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks.

**Service Providers** means authorised 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 Programme** means a programme that provides early identification of a potential Cardholder data compromise in your Cardholder Data Environment (CDE). See [Section 5, "Targeted Analysis Programme \(TAP\)"](#).

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

**Transaction** means a Charge, Credit, Cash Advance (or other cash access), or ATM Transaction completed by the means of a Card.

**Transaction Data** means all information required by American Express, evidencing one or more Transactions, including information obtained at the point of sale, information obtained or generated during Authorisation and Submission, and any Chargeback.

**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 Programme Attestation.

## Section 9

### Useful Websites

American Express Data Security: [www.americanexpress.com/datasecurity](http://www.americanexpress.com/datasecurity)

PCI Security Standards Council, LLC: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

EMVCo: [www.emvco.com](http://www.emvco.com)