American Express®
Data Security Operating Policy – United Kingdom

As a leader in consumer protection, American Express has a long-standing commitment to protect Cardmember Information, 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 on which encryption keys, Cardholder Data, or Sensitive Authentication Data (or both) are stored, processed, or transmitted.*

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

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

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

- store Cardholder Data only to facilitate American Express Card Transactions in accordance with, and as required by, the Agreement;
- comply with the current version of the Payment Card Industry Data Security Standard (PCI DSS) and PCI Pin Security Requirements no later than the effective date for implementing that version; and
- 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 4 below).

Section 2 – Data Incident Management Obligations

You must notify American Express immediately and in no case later than twenty-four (24) hours after discovery of a Data Incident.

To notify American Express, please contact the American Express Enterprise Incident Response Program (*EIRP*) at +1 (602) 537-3021 (+ indicates International Direct Dial "IDD" prefix, International toll applies), or email at EIRP@aexp.com. You must designate an individual as your contact regarding such Data Incident.

- You must conduct a thorough forensic investigation of each Data Incident. For Data Incidents involving 10,000 or more unique American Express Card account numbers (or otherwise at American Express's request), a PCI Forensic Investigator (***PFI***) must conduct this investigation.
- You must promptly provide to American Express all Compromised Card Numbers and the forensic investigation report of the Data Incident.
- You must work with American Express to rectify any issues arising from the Data Incident, including consulting with American Express about your communications to American Express 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.

Forensic investigation reports 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 providing a plan for remediating all PCI DSS deficiencies. Upon American Express's request, you shall provide validation by a Qualified Security Assessor (*QSA*) that the deficiencies have been remediated.

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

Section 3 – 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's other rights and remedies, under this Section 3.

American Express will not seek indemnification from you for a Data Incident (a) involving less than 10,000 unique Compromised Card Numbers or (b) if:

- you notified American Express of the Data Incident pursuant to Section 2 of this policy;
- 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.

You are liable for all other Data Incidents as set out in Appendix A at the end of this document.

Section 4 – IMPORTANT! Periodic Validation of Your Systems

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

There are four steps required to complete validation:

Step 1 – Enroll in American Express's Compliance Program under this Policy

Step 2 – Determine your Level and Validation Requirements

Step 3 – Determine the Validation Documentation that you must send to American Express

Step 4 – Send the Validation Documentation to American Express

Step 1 – Enroll in American Express's Compliance Program under this Policy

Level 1 Merchants, Level 2 Merchants, those Level 3 Merchants whom American Express has designated (as described below), Level EMV Merchants and all Service Providers, as described below, must enroll in American Express's compliance program under this policy by providing the full name, e-mail address, telephone number, and physical mailing address of an individual who will serve as their general data security contact. You must submit this information to Trustwave, which administers the program on behalf of American Express, by one of the methods listed in Step 4 below. You must notify Trustwave if this information changes, providing updated information where applicable.

American Express may require certain Level 3 Merchants to enroll in American Express's compliance program under this policy by sending them written notice. The designated Level 3 Merchant must enroll no later than 90 days following receipt of the notice.

Step 2 – Determine your Level and Validation Requirements

There are five levels for Merchants and two levels for Service Providers. Most levels are based on your volume of American Express Card Transactions.

Merchant Requirements

Merchants (not Service Providers) have five possible classifications regarding their level and validation requirements. For merchants, this is the volume submitted by their establishments that roll-up to the highest American Express merchant account level. See the Merchant table to determine validation documentation requirements.

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

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

Level 3 Merchant (designated) – Less than 50,000 American Express Card Transactions per year and has been designated by American Express as being required to submit validation documents. Designated Merchants are notified in writing by American Express at least 90 days before document submission is required.

Level 3 Merchant (non-designated) – Less than 50,000 American Express Card Transactions per year and has not been designated by American Express as being required to submit validation documentation.

Level EMV Merchant – who have not been involved in a Data Incident within the previous 12 months and also:

- Process 50,000 American Express Card Transactions or more per year
- At least 75% of all Transactions made by the Cardmember with the physical Card present
- Those transactions performed originate from EMV Chip-Enabled Devices

Merchant table

Level (defined above)	Validation Documentation (defined in Step 3 below)	Requirement
1	• Annual Onsite Security Assessment Report • Quarterly Network Scan	Mandatory
2	• Annual Self Assessment Questionnaire • Quarterly Network Scan	Mandatory
3 (Desig-nated)	• Annual Self Assessment Questionnaire • Quarterly Network Scan	Mandatory
3* (Non-Designated)	• Annual Self Assessment Questionnaire • Quarterly Network Scan	Strongly Recommended
EMV**	• PCI DSS Prioritized Approach Summary & Attestation of Compliance	Mandatory

*For the avoidance of doubt, Level 3 Merchants (Non-Designated) do not need to submit Validation Documentation, but nevertheless must comply with, and are subject to liability under all other provisions of this Data Security Operating Policy.

**Level EMV is not available for merchants that have had a Data Incident within twelve (12) months prior to the date of their Annual Assessment of Compliance.

Service Provider Requirements

Service Providers (not Merchants) have two possible classifications regarding their level and validation requirements. After determining the Service Provider level from the list below, see the Service Provider Table 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 Provider table

Level (defined above)	Validation Documentation (defined in Step 3 below)	Requirement
1	• Annual Onsite Security Assessment Report • Quarterly Network Scan	Mandatory
2	• Annual Self Assessment Questionnaire • Quarterly Network Scan	Mandatory

Step 3 – Determine the Validation Documentation that you must send to American Express

The following documents are required for different levels of Merchant and Service Provider as listed in the Merchant Table and Service Provider Table above.

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

- a QSA or
- you and certified by your chief executive officer, chief financial officer, chief information security officer, or principal and submitted annually to American Express on the applicable Attestation of Compliance (***AOC***).

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

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

Quarterly Network Scan – The Quarterly Network Scan is a process that remotely tests your Internet-connected computer networks and web servers for potential weaknesses and vulnerabilities. It must be performed by an Approved Scanning Vendor (ASV). You must complete and submit the ASV Scan Report Attestation of Scan Compliance (AOSC) or the executive summary of findings of the scan (and copies of the full scan, on request), quarterly to American Express. The AOSC or executive summary must certify that the results satisfy the PCI DSS scanning procedures, that no high risk issues are identified, and that the scan is passing or compliant (all Merchants except Level EMV; all Service Providers).

Annual Assessment of Compliance Milestones 1-4 of the PCI DSS Prioritized Approach Validation Documentation –The Annual Assessment of Compliance Milestones 1-4 of the PCI DSS Prioritized Approach is an examination of your equipment, systems, and networks (and their components) where Cardholder Data or Sensitive Authentication Data (or both) are stored, processed or transmitted. It must be performed by you and certified by your chief executive officer, chief financial officer, chief information security officer, or principal and submitted annually to American Express on the PCI DSS Prioritized Approach Summary & Attestation of Compliance (***PASAOC***). The PASAOC must certify compliance with milestones 1-4 of the PCI DSS Prioritized Approach and, upon request, include full details of such compliance. (Level EMV Merchants only).

Non Compliance with PCI DSS – If you are not compliant with the PCI DSS, then you must complete an AOC including "Part 4.Action Plan for Non-Compliant Status" and designate a remediation date, not to exceed twelve months following the date of the AOC, for achieving compliance. You must submit this AOC with the "Action Plan for Non-Compliant Status" to American Express by one of the methods listed in Step 4 below. You shall provide American Express with periodic updates of your progress toward remediation under the "Action Plan for Non-Compliant Status" (Level 1, Level 2, and Designated Level 3 Merchants; All Service Providers).

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.

Step 4 – Send the Validation Documentation to American Express

Level 1 Merchants, Level 2 Merchants, Designated Level 3 Merchants, Level EMV Merchants, and all Service Providers must submit the Validation Documentation marked "mandatory" in the tables in Step 2.

You must submit your Validation Documentation to Trustwave by one of these methods:

Secure Portal: Validation Documentation may be uploaded via Trustwave's secure portal at https://login.trustwave.com.

Please contact Trustwave at + 800 9000 1140 or +1 (312) 267-3208 or via email at AmericanExpressCompliance@trustwave.com for instructions on using this portal.

Secure Fax: Validation Documentation may be faxed to: +1 (312) 276-4019. (+ indicates International Direct Dial "IDD" prefix, International toll applies), Please include your name, trading name, the name of your data security contact, your address and phone number, and, for Merchants only, your 10-digit American Express Merchant number.

If you have general questions about the program or the process above, please contact Trustwave at + 800 9000 1140 or +1 (312) 267-3208 or via email at AmericanExpressCompliance@trustwave.com

Compliance and validation are completed at your expense. By submitting Validation Documentation, you represent and warrant to American Express that 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 notify you separately of the applicable deadline for each annual and quarterly reporting period.

Description (Currency GBP £)	Level 1 Merchant or Service Provider	Level 2 Merchant or Service Provider, Level EMV Merchant	Designated Level 3 Merchant only
A non-validation fee will be assessed if the Validation Documentation is not received by the first deadline.	£12,500	£2,500	£15
An additional non-validation fee will be assessed if the Validation Documentation is not received within 30 days of the first deadline.	£18,000	£5,000	
An additional non-validation fee will be assessed if the Validation Documentation is not received within 60 days of the first deadline.	£23,000	£7,500	

If American Express does not receive your mandatory Validation Documentation within 60 days of the first deadline, then American Express has the right to terminate the Agreement in accordance with its terms as well as impose the foregoing non-validation fees cumulatively on you.

Section 5 – Confidentiality

American Express shall take reasonable measures to keep (and cause its agents and subcontractors, including Trustwave, 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's 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:

i. is already known to American Express prior to disclosure;
ii. is or becomes available to the public through no breach of this paragraph by American Express;
iii. is rightfully received from a third party by American Express without a duty of confidentiality;
iv. is independently developed by American Express; or
v. 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 6 – 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 Web Sites

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

PCI Security Standards Council, LLC:

http://www.pcisecuritystandards.org

APPENDIX A: INDEMNITY CALCULATIONS

For a Data Incident involving American Express Card account numbers alone, you shall compensate American Express promptly by paying a Data Incident non-compliance fee not to exceed US$100,000 per Data Incident. For a Data Incident involving American Express Card account numbers with Sensitive Authentication Data, you shall compensate American Express promptly for:

- Incremental Fraud (defined below) within the Data Incident Event Window and
- Card monitoring and replacement costs of (i) US$1.00 per Card account number for 90% of the total number of Compromised Card Numbers and (ii) US$5.00 per Card account number for 10% of the total number of Compromised Card Numbers, respectively, and
- A Data Incident non-compliance fee not to exceed US$100,000 per Data Incident.

American Express shall calculate "Incremental Fraud" according to the following methodology:

Incremental Fraud = (X – Y) multiplied by Z, where:

X = Card issuers' total fraud losses excluding fraud chargebacks and losses from fraudulent Card applications on Compromised Card Numbers during the Data Incident Event Window divided by Card issuers' total Charge volume on Compromised Card Numbers during the Data Incident Event Window.

Y =
- Card issuers' total fraud losses excluding fraud chargebacks and losses from fraudulent American Express Card applications on non-Compromised Card Numbers during the Data Incident Event Window, divided by
- Card issuers' total Charge volume on non-Compromised Card Numbers during the Data Incident Event Window.

Z = Card issuers' total Charge volume on Compromised Card Numbers during the Data Incident Event Window.

American Express will exclude from its calculations of Incremental Fraud and Card monitoring and replacement costs any American Express Card account number that was involved in another Data Incident involving American Express Card account numbers with Sensitive Authentication Data, provided that American Express received notification of the other Data Incident within the twelve (12) months prior to the Notification Date. All calculations made by American Express under this methodology are final.

Merchants' 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.

APPENDIX B: 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

Attestation of Compliance, or 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.

Approved Scanning Vendor, or 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 Scan Compliance, or 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.

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

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***).

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 equipment or systems or payment processing solutions, and any other party to whom you may provide Cardmember Information 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 of American Express encryption keys, or at least one American Express Card account number in which there is:

- unauthorized access or use of Cardholder Data or Sensitive Authentication Data (or both) that are stored, processed, or transmitted on your equipment, systems, and/or networks (or the components thereof);
- use of such Cardholder Data or Sensitive Authentication Data (or both) 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 Cardholder Data or Sensitive Authentication Data.

Data Incident Event Window means the period that begins 365 days prior to the Notification Date and ends 30 days after the Notification Date.

Designated Level 3 Merchant means Merchants who have been notified by American Express that they are required to participate in the American Express PCI Compliance program and report their compliance status.

EMV Specifications means the specifications issued by EMVCo, LLC, which are available at 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 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

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

Level 2 Merchant means a merchant that submits 50,000 to 2.5 million American Express Card Transactions per year.
Level 3 Merchant (Designated) means a merchant which has been notified by American Express that they are required to participated in the American Express PCI Compliance program and report their compliance status.

Level 3 Merchant (Non-Designated) means a merchant that submits less than 50,000 American Express Card Transactions per year and has not been designated by American Express.

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

Level EMV Merchant means a merchant which has not been involved in a Data Incident within the previous 12 months and also:

- Process 50,000 American Express Card Transactions or more per year; and
- At least 75% of the merchant's total Transaction count are made with the physical Card present and originate on Point of Sale Systems compliant with American Express EMV Specifications.

Milestones 1-4 means priorities assigned to PCI DSS requirements by the PCI Prioritised Approach, which is available at https://www.pcisecuritystandards.org.

Notification Date means the date, designated by American Express, that issuers receive notification of the Data Incident.

Payment Application has the meaning given to it in the then current Glossary of Terms for Payment Card Industry Payment Application Data Security Standard, which is available at https://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 https://www.pcisecuritystandards.org.

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

PCI DSS Prioritized Approach means the PCI DSS document made available at https://www.pcisecuritystandards.org/security_standards/prioritized.php.

PCI DSS Prioritized Approach Summary & Attestation of Compliance, or PASAOC means a declaration of the status of your compliance with the PCI DSS Prioritized Approach, in the form provided by the Payment Card Industry Security Standards Council, LLC.

PCI Forensic Investigator, or 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 https://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 https://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.

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

Qualified Security Assessor, or QSA, means an entity that has been qualified by the Payment Card Industry Security Standards Council, LLC to validate adherence to the PCI DSS.

Self-Assessment Questionnaire, or 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, and any other providers to Merchants of point of sale equipment, software, or systems, or other payment processing solutions or services.

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 EMV Attestation.