American Express Data Security Operating Policy for Merchants in the 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, 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 ("**you**") share our concern and requires, as part of your responsibilities, that you comply with the data security provisions in your agreement to accept the American Express® Card, ("**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 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 I – Standards for Protection of Cardholder Data and Sensitive Authentication Data

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

(i) store Cardholder Data only to facilitate American Express Card transactions in accordance with, and as required by, the Agreement and

(ii) comply with the current version of the Payment Card Industry Data Security Standard ("PCI DSS") no later than the effective date for implementing that version.

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 to 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:

(i) you notified American Express of the Data Incident pursuant to Section 2 of this policy,

(ii) you were in compliance at the time of the Data Incident with the PCI DSS or, if you are a Level EMV Merchant, you were in compliance at the time of the Data Incident with at least the PCI DSS requirements identified in milestones 1-4 of the PCI DSS Prioritised Approach (as determined by the PFI's investigation of the Data Incident), and

(iii) 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 follows. 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 number for 90% of the total number of Compromised Card Numbers and (ii) US$5.00 per Card 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 = (i) 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 (ii) Card issuers' total charge volume on Compromised Card Numbers during the Data Incident Event Window.

Y = (i) 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 (ii) 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.

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 (or both) are stored, processed or transmitted.

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

Level EMV, Level 1, and Level 2 merchants, as described below, must enrol 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 3 below. You must notify Trustwave if this information changes, providing updated information where applicable.

Step 2 – Determine your Merchant Level and Validation Requirements

There are four Merchant Levels for merchants. Most Merchant Levels are based on your volume of American Express Card transactions submitted by your establishments that roll-up to the highest American Express merchant account level. You will fall into one of four Levels specified in the table below.

Merchant Level	Definition	Validation Documentation	Requirement
EMV	50,000 American Express Card transactions or more per year, of which at least 75% are EMV Transactions	Annual Assessment of Compliance Milestones 1-4 of the PCI DSS Prioritised Approach	Mandatory
1	2.5 million American Express Card transactions or more per year; or any merchant that American Express otherwise deems a Level 1 merchant	Annual Onsite Security Assessment Report, and Quarterly Network Scan	Mandatory
2	50,000 to 2.5 million American Express Card transactions per year	Annual Self Assessment Questionnaire and Quarterly Network Scan	Mandatory
3	Less than 50,000 American Express Card transactions per year	Annual Self Assessment Questionnaire and Quarterly Network Scan	Strongly Recommended*

*Level 3 Merchants need not submit Validation Documentation, but nevertheless must comply with, and are subject to liability under all other provisions of this Data Security Operating Policy.

Determine your Merchant Level and the Validation Documentation that you must send to American Express.

Annual Assessment of Compliance Milestones 1-4 of the PCI DSS Prioritised Approach Validation Documentation – The Annual Assessment of Compliance Milestones 1-4 of the PCI DSS Prioritised 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 Prioritised Approach Summary & Attestation of Compliance ("PASAOC"). To fulfil validation obligations under this policy, the PASAOC must certify compliance with milestones 1-4 of the PCI DSS Prioritised Approach and, upon request, include full details of such compliance.

Annual Onsite Security Assessment Validation Documentation – 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 (i) a QSA or (ii) 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"). To fulfil validation obligations under this policy, the AOC must certify compliance with all requirements of the PCI DSS and, upon request, include copies of the full report on compliance

Annual Self Assessment Questionnaire Validation Documentation – 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. To fulfil validation obligations under this policy, 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.

Quarterly Network Scan Validation Documentation – 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. To fulfil validation obligations under this policy, 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.

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" or, if you are a Level EMV Merchant, the PASAOC, and designate a remediation date, not to exceed twelve months following the date of the AOC, or the PASAOC, as applicable, for achieving compliance. You must submit this AOC with "Action Plan for Non-Compliant Status" or the PASAOC, if you are a Level EMV Merchant, to American Express by one of the methods listed in Step 3 below. You shall provide American Express with periodic updates of your progress toward remediation under the "Action Plan for Non-Compliant Status" or the PASAOC, as applicable. 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 3 – Send the Validation Documentation to American Express

Level EMV, Level 1 and Level 2 Merchants must submit the Validation Documentation marked "mandatory" in the table in Step 1.

- Level EMV Merchant's Validation Documentation must include the Annual Assessment of Compliance Milestones 1-4 of the PCI DSS Prioritised Approach, as described above.
- Level 1 Merchant's Validation Documentation must include the AOC from the Annual Onsite Security Assessment Report and the AOSC or executive summaries of findings of the Quarterly Network Scans, as described above.
- Level 2 Merchant's Validation Documentation must include the AOC from the SAQ and the executive summaries of findings of the Quarterly Network Scans, as described above.
- Level 3 Merchants are not required to submit Validation Documentation (but must comply with, and are subject to liability under, all other provisions of this policy).

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. Please contact Trustwave at +800-9000-1140 (+ indicates International Direct Dial "IDD" prefix, International toll free,) or via email at AmericanExpressCompliance@trustwave.com for instructions in using this portal.

Secure Fax: Validation Documentation may be faxed to: +1 (312) 276-4019 (International toll applies). Please include your name, Trading Name, 10-digit American Express merchant number, the name of your data security contact, your address, and phone number.

Mail: Validation Documentation may be copied in an encrypted format on a compact disc. Place in an envelope marked "Mandatory" and mail to:

American Express - DSOP Compliance Program
c/o Trustwave
70 West Madison, Suite 1050
Chicago, IL 60602
USA

E-mail the encryption key required to decrypt the Validation Documentation along with your name, Trading name, 10-digit American Express merchant number, name of your data security contact, your address, and phone number to Trustwave at AmericanExpressCompliance@trustwave.com

If you have general questions about the program or the process above, please contact Trustwave at +800-9000-1140 (International toll free) 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 fulfil 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.

	Level 1	Level 2, Level EMV
A non-validation fee will be assessed if the Validation Documentation is not received by the first deadline.	£12,500	£2,500
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.

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 5– 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:
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 (i) 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 (ii) 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 Information means information about American Express cardmembers and Card transactions, including names, addresses, card account numbers, and card identification numbers ("CIDs").

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.

Data Incident means an incident involving at least one American Express Card account number in which there is (i) 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); (ii) use of such Cardholder Data or Sensitive Authentication Data (or both) other than in accordance with the Agreement; and/or (iii) 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 (or both).

Data Incident Event Window means the period that begins 365 days prior to the Notification Date and ends 33 days after the Notification Date.

EMV Specifications means the specifications issued by EMVCo that define a set of requirements to ensure interoperability between chip cards and terminals on a global basis. The specifications 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.

Level EMV Merchant means a merchant that has 50,000 American Express Card transactions or more per year, of which at least 75% are EMV Transactions.

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

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

PCI DSS Prioritised Approach means the PCI DSS Prioritised Approach available at https://www.pcisecuritystandards.org.

PCI DSS Prioritised Approach Summary & Attestation of Compliance, or PASAOC means a declaration of the status of your compliance with the PCI DSS Prioritised 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.

Processor means a service provider to merchants who facilitates 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.

Validation Documentation means the AOC rendered in connection with an Annual Online Security Assessment or SAQ, the PASAOC rendered in connection with an Annual Assessment of Compliance Milestones 1-4 of the PCI DSS Prioritised Approach, the AOSC and executive summaries of findings rendered in connection with Quarterly Network Scans.