American Express Data Security Operating Policy for Merchants

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 data 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.

Cardmembers rely on American Express for the highest level of service and protection. In continuously addressing security issues, we have developed this Data Security Operating Policy and are working with Merchants to help them establish appropriate security programs.

American Express knows that 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 (Card Acceptance Agreement), which includes this policy. These requirements apply to all your equipment, systems, and networks on which American Express Cardmember Information is processed, stored, or transmitted.

Section I – Data Security Standards for Merchants

Merchants must, and they must cause their Covered Parties, to:

(i) store Cardmember Information only to facilitate Card transactions in accordance with their Card Acceptance Agreements; and

(ii) comply with the current version of the Payment Card Industry Data Security Standard (PCI Standard, which is available at www.pcisecuritystandards.org) no later than the effective date for implementing that version.

Covered Parties means any or all of a merchant's employees, agents, representatives, subcontractors, Processors, Service Providers, providers of its point of sale equipment or systems or payment processing solutions, and any other party to whom it may provide Cardmember Information access in accordance with its Card Acceptance Agreement.

Section 2 – Duty to Notify American Express

Merchants must notify American Express immediately if they know or suspect that Cardmember Information has been accessed or used without authorisation or used other than in accordance with their Card Acceptance Agreement. Merchants must engage at their sole cost a third party forensic investigator to conduct a thorough audit of such data incident, or they must provide (and obtain any waivers necessary to provide) to American Express and its forensic investigators and auditors, on request and at the merchant's sole cost, full cooperation and access to conduct a thorough audit of such data incident. Merchant's shall promptly provide to American Express, all Card account numbers related to the data incident and audit reports of the data incident. Merchants must work with American Express to rectify any issues arising from the data incident, including consulting with American Express about their communications to Cardmembers affected by the data incident and providing (and obtaining any waivers necessary to provide) to American Express all relevant information to verify their ability to prevent future data incidents in a manner consistent with their Card Acceptance Agreement. Audits must include forensic reviews and reports on compliance, as well as any and all information related to the data incident, and they must identify the cause of the data incident and confirm whether or not the Merchant was in compliance with the PCI Standard at the time of the data incident. We may contact a third party security assessor to begin a forensic investigation or site certification.

Merchant's indemnity obligations to American Express under their Card Acceptance Agreement include, without waiving any of American Express's other rights and remedies, liability for all fraudulent transactions related to such data incidents and all costs, fees, and expenses (including claims from third parties and all costs incurred by American Express related to the notification of Cardmembers, cancellation and reissuance of Cards, fraud monitoring, reasonable legal fees and dis-

bursements, and costs of investigation, litigation, settlement, judgment, interest, and penalties) that American Express incurs as a result of such data incidents unless:

(i) the merchant notifies American Express pursuant to this section;

(ii) the merchant is and was in compliance at the time of the data incident with this Data Security Operating Policy; and

(iii) the data incident was not caused by the wrongful conduct of the merchant or one of its employees or agents.

Contact your Client Manager or call the American Express Merchant Help Desk on 01273 67 55 33 if you believe that Cardmember Information has been compromised. Please have your American Express Merchant Number and your bank account details with you when you call.

Section 3 – IMPORTANT! Demonstration of Compliance with Data Security Operating Policy

Merchants must take the following steps to demonstrate their compliance with this Data Security Operating Policy, annually or quarterly as described below (each such period, a reporting period).

Step 1 – Determine your Merchant Level and Validation Requirements

Most Merchant Levels are based on a Merchant's volume of American Express Card transactions submitted by its Establishments that roll-up to the highest American Express account level. Merchants fall into one of three levels specified in the table below.

Level	Definition	Validation Documentation	Requirement
1	2.5 million American Express Card transactions or more per year; or any merchant that has had a data incident; or any merchant that American Express otherwise deems a Level 1	Annual Onsite Security Audit Report, and Quarterly Network Scan	Mandatory
2	50,000 to 2.5 million American Express Card transactions per year	Quarterly Network Scan and Annual Self-Assessment	Mandatory
3	Less than 50,000 American Express Card transactions per year	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 documents that you must send to American Express in order to validate your compliance with this policy.

Annual Onsite Security Assessment Validation Documentation

The Annual Onsite Security Assessment is a detailed onsite examination of merchant equipment, systems, and networks (and their components) where Cardmember Information is processed, stored, or transmitted. It must be performed by:

(i) a Qualified Security Assessor (QSA), listed below; or

(ii) the merchant and certified by the chief executive officer, chief financial officer, or principal of the merchant.

Merchants must complete and submit the summary of the findings of this assessment (and copies of the full report on compliance, on request) annually to American Express.

For a Merchant to be deemed compliant with this Data Security Operating Policy, the summary must certify the Merchant's compliance with all requirements of the PCI Standard. A list of QSAs is available at www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

Quarterly Network Scan Validation Documentation

The Quarterly Network Scan is a process that remotely tests a merchant's internet-connected computer networks and web servers for potential weaknesses and vulnerabilities. It must be performed by an Approved Scanning Vendor (ASV), listed below. Merchants must complete and submit the summary of the findings of the scan (and copies of the full scan, on request) quarterly to American Express. For a Merchant to be deemed compliant with this Data Security Operating Policy, the summary must certify that there are no high risk issues. A list of ASVs is available at www.pcisecuritystandards.org/pdfs/asv_report.html

Annual Self-Assessment Questionnaire

The Payment Card Industry (PCI) Self-Assessment Questionnaire is to be used by a Merchant as a 'checklist' to ensure that critical security measures are in place to safeguard and protect Cardmember Information. It should address any system(s) or system component(s) involved in processing, storing, or transmitting Cardmember Information. Merchants must complete and submit the completed Questionnaire annually to American Express. For a Merchant to be deemed compliant with this Data Security Operating Policy, the Questionnaire must certify the Merchant's compliance with all requirements of the PCI Standard. The

Self-Assessment Questionnaire is available at www.pcisecuritystandards.org/tech/supporting_documents.htm

Step 2 – Send the Validation Documentation to American Express

Level 1 and Level 2 Merchants must submit the Validation Documentation marked "mandatory" in the table in Step 1, in an encrypted format, via compact disc, to American Express at the address below:

American Express Payment Services Limited
GNO Data Security Unit
PO Box 54886
London, SW1W 0YW
United Kingdom

- Level 1 Merchants' Validation Documentation must include summaries of findings of the Annual Onsite Security Assessment Report and Quarterly Network Scan report, as described above.
- Level 2 Merchants' Validation Documentation must include summaries of findings of the Quarterly Network Scan and a completed PCI Self Assessment Questionnaire, 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).

The encryption key required to decrypt the Validation Documentation, as well as the Merchant name, the Merchant's data security contact including name, address and phone number, and the Merchant's 10-digit American Express number, must be e-mailed to: AmericanExpressDataSecurityEMEA@aexp.com

Compliance and validation is completed at the Merchant's expense. By submitting Validation Documentation, Merchants represent and warrant to American Express that they 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-Validation Fees and Termination of Card Acceptance Agreement

Merchants will be assessed for non-validation fees and their Card Acceptance Agreement may also be terminated if they do not fulfil these requirements or fail to provide the mandatory Validation Documentation to American Express by the applicable deadline. American Express will notify merchants separately of the applicable deadline for each reporting period.

	Level 1	Level 2
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 a Merchant's mandatory Validation Documentation within 60 days of the first deadline, then American Express may terminate the merchant's Card Acceptance Agreement in accordance with its terms as well as impose the foregoing non-validation fees on the Merchant.

Confidentiality Commitment

American Express shall take reasonable measures to keep a Merchant's report on compliance, including its summary of findings rendered in connection with an Annual Onsite Security Assessment, PCI Annual Self-Assessment Questionnaire and summary of findings rendered in connection with a Quarterly Network Scan (such documents called Validation Documentation) in confidence and not disclose the Validation Documentation to any third party (other than its agents, representatives, service providers, and subcontractors) for a period of two 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 by a merchant;

ii) is or becomes available to the public through no breach of this paragraph by American Express;

ii) 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 4 – Disclaimer

Except as otherwise specified in this policy, a Merchant's compliance with this Data Security Operating Policy shall not in any way relieve its indemnity obligations to American Express under its Card Acceptance Agreement, nor relieve or decrease its liability in any way. Merchants are responsible at their sole expense for providing additional data security measures that they deem necessary to protect their particular data and interests. American Express does not in any way represent or warrant that the measures contained in the Card Acceptance Agreement or this policy are sufficient or adequate to protect Merchants' particular data and interests.

American Express hereby disclaims any and all representations, warranties, and liabilities with respect to this Data Security Operating Policy, the PCI Standard, and the designation and performance of QSA or ASV (or both), whether express, implied, statutory, or otherwise, including any warranty or fitness for a particular purpose.

Useful Web Sites

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

PCI Security Standards Council, LLC for:

- PCI Data Security Standards copy
- Self Assessment Questionnaire copy
- List of Qualified Security Assessors
- List of Approved Scanning Vendors

www.pcisecuritystandards.org