# American Express Website Compromise Checklist

## Merchant Overview

Please provide the following information about your cardholder data environment (CDE). This information is necessary to understanding potential scope if a data incident is confirmed.

Note: Per the Card Acceptance Agreement (CAA) and the Data Security Operating Policy (DSOP), American Express must be notified of a data incident within 72 hours of discovery. Notification of a data incident doesn't automatically result in fees.

Company Name:

| | | | |
|---|---|---|---|
| Card Payment methods accepted (Check all that apply) | ☐EMV with Signature<br>☐EMV with PIN<br>☐E-Commerce<br>☐Phone/Mail order<br>☐ Other | | |
| Ecommerce urls (if applicable): | | | |
| Do you have multiple locations? | ☐No<br>☐Yes | If Yes, please list: | |
| Are you a franchise? | ☐No<br>☐Yes | If Yes, who is compromised? | ☐ Corporate owned locations<br>☐ Franchisee owned locations |
| Do you have Data Breach or Cyber Insurance? | ☐No<br>☐Yes | If Yes, under what circumstances can it be invoked? | |
| Do you use a third-party vendor or service provider (e.g. shopping cart, payment processor, payment gateway, hosting provider) ? | ☐No<br>☐Yes | If Yes, please list all and the service provided: | |

High level overview of Card payment acceptance processes:

| Response Actions | Completion Date |
|---|---|
| The following is a list of actions to help your internal resources find data security gaps most likely to be associated with an ecommerce Cardholder data compromise. If, despite best efforts, internal resources are unable to identify and address the source of a potential data compromise, you may be required to engage a PCI Forensics Investigator.<br><br>Note: Failure to take action may result in non-compliance fees and/or termination of Card acceptance. | |
| **Malware:** Verify anti-virus and malware detection scans are running at least daily. Address findings as applicable.<br>Note: *Only use scans from a reliable source. Anti-virus scan capability is integrated into the SecureTrust PCI Manager account provided by American Express. Contact AmericanExpressCompliance@securetrust.com .*<br>**Notes/Findings/Comments:** | |
| **Malware:** Verify that all recommended security headers are hardened on your website and, as applicable, ecommerce pages.<br>Note: *Cross-site scripting is, still, the number one method used by hackers to gain access to sensitive information on ecommerce pages.*<br>**Notes/Findings/Comments:** | |

| | |
|---|---|
| **Malware:** Remove or disable ads running on any page of your website and ecommerce pages that collect sensitive information from cardholders.<br>Note: *Malvertising is a known risk associated with the use of ad networks. Talk to any/all ad networks interacting with your website or ecommerce pages to validate their security practices.*<br>**Notes/Findings/Comments:** | |
| **Malware:** Review all scripts and tags running on your website and ecommerce pages to validate the legitimacy of all code. Be especially mindful of any queries that are triggered when the CVV code is entered and/or send data to a database or website. Remove/replace any unapproved scripts, tags, urls and/or commands.<br>Note: *Hackers often inject custom code or spoofed urls into complex javascript strings. This is especially prevalent when using open source solutions.*<br>**Notes/Findings/Comments:** | |
| **Unpatched Systems:** Run an external vulnerability scan on all internet facing networks. Address findings as applicable.<br>Note: *External vulnerability scan capability is integrated into the SecureTrust PCI Manager account provided by American Express. Contact AmericanExpressCompliance@securetrust.com .*<br>**Notes/Findings/Comments:** | |
| **Unpatched Systems:** Install all critical patches to your CDE (e.g. POS, payment application, shopping cart, network).<br>Note: *Critical patches should always be applied within one month of release. It is recommended that critical patches applicable to your website or ecommerce environment be installed within 24 hours, if possible.*<br>**Notes/Findings/Comments:** | |
| **Outdated Systems:** If you are running a version of any applications and/or software (e.g. payment application, shopping cart, jquery, programming code, operating system, email) in your CDE that is outdated and/or no longer supported by the developer, install necessary upgrades.<br>Note: *Expenses associated with necessary upgrades can be easily justified when compared to the resultant cost of brand damage and noncompliance fees when a data breach crosses indemnity thresholds.*<br>**Notes/Findings/Comments:** | |
| **Weak Passwords:** Change all passwords and, where possible, implement multi-factor authentication for all accounts associated with your network (e.g. POS, router, user logins, admin access).<br>Note: *This step is recommended for any/all locations and/or franchisees using one or more of the same account types as you do.*<br>**Notes/Findings/Comments:** | |
| **Remote Access:** Change passwords and, where possible, implement multi-factor authentication for your network (e.g. firewall, administration), website and/or ecommerce solution (e.g. web host, shopping cart, administration, LogMeIn, ConnectWise) user ids.<br>**Notes/Findings/Comments:** | |
| **Remote Access:** Update remote access configuration settings (e.g. change from default, set business hours and/or markets, multi-attempt lockout) to restrict access and, where possible, implement multi-factor authentication.<br>**Notes/Findings/Comments:** | |
| **Other:** Contact any/all payment vendors or service providers supporting your Card acceptance capabilities. They may have experienced a data security incident during highlighted timeframe or they may be able to help you address any common misconfigurations of their products.<br>**Notes/Findings/Comments:** | |

## Current PCI Compliance Validation Status

Please provide the following information about your current PCI DSS compliance status.

Note: The Payment Card Industry Data Security Standard (PCI DSS) is applicable to all entities that accept, store or process Card payment data.

| | | |
|---|---|---|
| When was the last external vulnerability scan completed, if required? | Completed By:<br>Date: | ☐Compliant<br>☐Non-compliant<br>☐Other |
| When was the last PCI Compliance validation completed (i.e. ROC, SAQ, other)? | Validation Type: | ☐Compliant<br>☐Non-compliant |

|  |  |  |
|---|---|---|
|  | Completed By:<br>Date: | ☐Other |
| Do you have the following documents describing your current CDE? (check all that apply) | ☐ Network diagram<br>☐ Card data flow<br>☐ List of devices connected to your CDE<br>☐ Payment Vendor or Service Provider contacts & PCI Compliance status<br>☐ Written acknowledgement that payments are wholly outsourced, if applicable |  |
| Did you find and address any issues in your cardholder data environment as you completed the Response Actions? | ☐No<br>☐Yes | Explain: |
| Has any other acquirer, processor, Card brand or law enforcement contacted you regarding suspicion of a data incident or CPP within the past six months? | ☐No<br>☐Yes | Contacted By:<br>Date of Contact:<br>Explain: |
| Have you engaged a forensics investigator (PFI) or Qualified Security Assessor (QSA) to evaluate your CDE within the past six months? | ☐No<br>☐Yes | Company Name:<br>Date Engaged:<br>Completion Date (if applicable):<br>Explain: |
| Have you confirmed the loss of Card data from your environment within the last six months? | ☐No<br>☐Yes | Explain: |

## Acknowledgement of Status

Signatory confirms the actions on this checklist was completed to the best of my ability and knowledge and all information provided fairly represents my observations.

Signature of Merchant Executive Officer

Date

Print Merchant Executive Officer Name

Title