MERCHANT SERVICES

Merchant Investigations
Frequently Asked Questions

COMMON POINT OF PURCHASE

What is a Common Point of Purchase (CPP) Investigation?

A CPP investigation is initiated when multiple fraudulent transactions are reported to the Payment Brands and determined to have originated from a common location. The "common location" becomes the CPP, the last location that the card was successfully authorized before being used fraudulently. This location may have suffered a cardholder data compromise.

Did the fraud take place at my location?

No. The CPP merchant location is where the cardholder data was likely stolen, or where a data security breach may have occurred. The stolen card data is then used for fraudulent purchases at other merchant locations.

Who reported the fraudulent activity?

CPP locations are reported by the Payment Brands (American Express, Visa®, MasterCard®, Discover®) to law enforcement and issuing banks. Once reported, the appropriate payment brand examines the claim to determine whether a CPP or forensic investigation is necessary.

What do I do if my business is reported as a CPP location?

If your business is reported as a CPP location, Chase will contact you. The payment brand involved will then provide a questionnaire for you to complete, as well as details from the report that will assist you with your own internal investigation. You will be given a deadline for submitting the questionnaire to Chase.

What will Chase do if my business is reported as a CPP location?

Chase will notify their merchant that their location has been identified in a CPP analysis by a Payment Brand. Chase will coordinate communication between their merchant and the reporting Payment Brand and review the completed questionnaire and forward it to the Payment Brand. The Payment Brand will determine, based on the responses to the CPP questionnaire, whether a cardholder data compromise may have occurred.

How do I start my CPP investigation? What am I looking for?

Security breaches can appear in different forms. Staying alert for the following suspicious activities can help identify potential risks:

- Validate that virus scan signature files are current and recent runs are clean
- Look at network logs for unusual inbound or outbound access from unknown IP addresses
- Review system logs for system access outside of normal business hours
- Unknown files, software and devices installed on your systems
- Antivirus programs malfunctioning or becoming disabled
- Unknown applications configured to launch automatically upon your system reboot
- Presence of .zip, .rar, .tar and other types of unidentified compressed files containing cardholder data

What are my notification requirements should I detect a potential compromise of my Payment Environment?

The requirements for a merchant to promptly notify Chase when they suspect a potential compromise of their payment environment are defined in your merchant agreement. It states that if at any time either party determines or suspects that Card Information has been compromised, such party shall notify the other promptly (and in no event later than 48 hours after such determination or suspicion) and assist in providing notification to such parties as may be required by applicable law or Card Network Rules.

J.P.Morgan

Merchant Investigations
Frequently Asked Questions, cont'd

Chase sent me a file that looks like cardholder data. What is this?

This data is the transaction detail file that the Payment Brand identified in their CPP analysis. This transaction data is the last successful authorization for the account that was used at your location before it was used fraudulently at another location. This data is provided to assist you with your investigation of the CPP notification.

PAYMENT CARD INDUSTRY (PCI) COMPLIANCE

What is PCI Compliance?

All merchants who store, process or transmit cardholder data must comply with the Payment Card Industry Data Security Standards (PCI DSS) to protect cardholder data. A merchant's Annual PCI validation requirements are determined by their Merchant Level. In addition, if a merchant uses a service provider that stores, processes or transmits cardholder data on their behalf, the service provider must also comply with PCI DSS requirements. When a CPP investigation is initiated by a Payment Brand, the merchant is required to provide validation documentation of PCI compliance.

What is an Approved Scanning Vendor (ASV) Scan?

An Approved Scanning Vendor (ASV) is an organization with a set of security services and tools ("ASV scan solution") to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS Requirement 11.2.2. The scanning vendor's ASV scan solution is tested and approved by PCI SSC before an ASV is added to PCI SSC's List of Approved Scanning Vendors. The scan produced by this service identifies potential vulnerabilities to the scanned environment that could be exploited to compromise security measures.

DATA COMPROMISE

What is a Cardholder Data Compromise?

Cardholder data compromise occurs when information from a consumer credit card is released externally without the consumer's knowledge. This can be caused by a malicious employee or a breach of the merchant's payment system. When a data compromise occurs, it is critical to immediately identify the root cause of the event to contain the damage, limit financial loss, and protect customer data. Merchants will be required to produce an accurate record of events for authorities and the Payment Brands.

How is a Cardholder Data Compromise identified?

Any suspicion of potential cardholder data compromise is reported to the Payment Brands (Visa® MasterCard® Discover®) by law enforcement, issuing banks, and/or you the merchant by notifying your Acquirer.

What is a request for a PFI investigation?

When the Payment Brands have evidence that a compromise of a Merchant's payment environment has occurred, they will request that the environment be investigated by a PCI approved Forensic Investigation (PFI) firm. The current list of PCI approved PFI firms is located at: https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators.

Why must I engage a PFI firm when I already have a relationship with a Security Firm who can conduct an Incident response?

The Payment Card Industry Security Standards Council (PSI/SSC) has established a rigorous training validation program to insure only knowledgeable investigators respond to a compromise of a payment environment. The PCI/SSC PFI program also has established thorough investigation procedures and reporting standards to insure that all issues potentially impacting the payment environment are identified and remediated as quickly as possible.

J.P.Morgan

Merchant Investigations
Frequently Asked Questions, cont'd

What happens during a Cardholder Data Compromise investigation?

1. *Forensic investigation* – Upon review of an incident report, Visa or MasterCard may request that the merchant engage a PCI Forensic Investigator (PFI) to perform a forensic investigation within a specific time frame. Conducting a forensic investigation helps determine if there is evidence or risk of a compromise, and the time period of the compromise.
2. *Report findings* – When the investigation is complete, the PFI will provide a forensic report to the merchant and the report will be shared with Chase and all affected Payment Brands. Chase will coordinate a review of the findings and the required follow-up actions identified in the report.
3. *Accounts at risk* – The PFI and Chase will provide all affected Payment Brands with the cardholder accounts that were processed during the at-risk time period. The Payment Brands will then notify the corresponding Issuers. Issuers are given a deadline to report any related fraud to the payment brands.
4. *Expenses, fines and liabilities* – The merchant is responsible for bringing in the PFI, if required. The Payment Brands will assess separate fines for lack of compliance, which led to the breach. In some cases, there are also assessments for incremental fraud and for monitoring or re-issuing cardholder accounts.
5. *Compliance with the Payment Card Industry Data Security Standard* – Any entity that has suffered a hack or attack is required to validate PCI compliance. The forensic investigation will not close until the merchant has provided a Report of Compliance or Self Assessment Questionnaire, in addition to Quarterly Network Scans.

What is Skimming?

Skimming is the unlawful transfer of cardholder data to another source for fraudulent purposes. This may be a small handheld skimming device used by an employee or small electronic skimming equipment inserted into a terminal. Merchants should educate their employees to be aware of alterations to payment devices or rogue devices that can be used for skimming and notify management when discovered.

What is a Network Intrusion?

A network intrusion (breach) occurs when unauthorized network access into the payment environment occurs with the intent to extract cardholder data. The Payment Security Investigation Form will expose possible vulnerabilities that may contribute to a network intrusion. If a network intrusion has occurred, the magnitude of the event may be significantly greater than that of a skimming event. Counterfeit cards can be produced in larger volume with the data extracted from a network intrusion, thus producing more fraudulent losses. If the compromise is determined to be a result of a network intrusion, the CPP investigation will be escalated to a forensic investigation. To avoid network intrusions, merchants utilizing a non-compliant payment application and who are not compliant with the Payment Card Industry Data Security Standard (PCI DSS) should immediately upgrade to a PA DSS/PABP compliant payment application and pursue PCI DSS compliance.

For additional information regarding PCI and Payment Security:

- Payment Card Industry Security Standards Council: https://www.pcisecuritystandards.org
- PCI Glossary of Terms, Abbreviations, and Acronyms: https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf
- PCI Guidance on responding to a Data Breach: https://www.pcisecuritystandards.org/documents/Responding_to_a_Cardholder_Data_Breach.pdf
- MasterCard: https://www.mastercard.us/en-us/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI.html
- Visa: https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf
- If you have questions regarding PCI compliance, email the PCI Compliance Team at PCI_Compliance@chase.com
- If you have further questions, please contact your Account Executive, or email the Merchant Investigations Team at PTI-DataCompromise@chase.com

J.P.Morgan