



The Anatomy of a Data Security Breach

Over the past 25 years, amazing advancements in technology have occurred allowing restaurant operators to increase speed of service, improve guest experience, and make effective real-time decisions from increased visibility into restaurant operations. These advancements have freed restaurant operators to focus on the areas of their business that matter the most: driving operational efficiencies and squeezing bottom lines for as much profit as possible. Unfortunately, similar advancements have occurred that threaten the sensitive data that restaurant operators process, transmit and store within their businesses. Criminals targeting the restaurant industry are getting more and more sophisticated. Criminals are leveraging technology like never before, and their actions can have serious consequences for a restaurant operator. They can damage a restaurant's reputation, destroy customer loyalty and even put a restaurant out of business.

Many restaurant operators are unaware of the actions taken when a payment card brand, like Visa or MasterCard, or an issuing bank, like Wells Fargo or Capital One, suspects a business may have been the victim of a data security breach. This white paper is designed to provide restaurant operators with a more detailed outline of the steps taken to discover, validate and resolve a data security breach if it occurs.



How Identification of a Potential Data Security Breach Occurs

The sequence of action begins when a data security breach is suspected and is escalated to the payment card brands. This escalation can occur in a wide variety of ways, such as:

- A consumer identifies fraudulent charges on his or her credit card statement and notifies the issuing bank. The issuing bank in turn notifies the card brand of the potential incident, the card brand starts analyzing the other reported charge-back's in its system to identify a common point of purchase where multiple payment cards were used for legitimate use and subsequent fraud.
- A restaurant operator or its acquiring bank notifies a payment card brand directly of an incident involving unauthorized access to the restaurant operator's network which may hold sensitive data, or the theft of hardware or merchant receipts.

Once a common point of purchase is identified, the payment card brand sends a notification to the business's acquiring and/or issuing bank. The bank, in turn, notifies the business that a potential data security breach occurred at that business.

Moving from Identification to Investigation

Once identified as the location of a potential data security breach, the suspected business undergoes an initial investigation from a bank investigator who fills out a questionnaire regarding the security of the business. This information must be sent directly to the payment card brands within 3 to 5 days of identifying the potential data security breach. These results are analyzed to determine if enough evidence exists to move forward with a full forensics investigation. If the payment card brand believes enough evidence has been found, the business is notified that a full forensic investigation must be conducted by a Qualified Incident Response Assessor (QIRA).

Upon receipt of the investigation notification, a business must

identify a QIRA within 72 hours of notification. The business must also ensure that the QIRA is engaged within 10 business days with a contract signed, and the onsite investigation must occur within five business days after the contract agreement is signed. Compromised businesses should engage the QIRA directly, however, the payment card brands have the right to engage a QIRA to perform any investigations as it deems appropriate. The payment card brands will pass all investigative costs to the compromised business in addition to any fines that may be applicable.

On average, active investigations can take anywhere from 30-90 days, depending on the complexity of the investigation. The average costs of hiring a QIRA range between \$10,000 - \$25,000. During this time, the business cannot process payments electronically and must move to dial up process or other means to process payments. The business also has to lock down its compromised payment processing systems and it cannot be touched for support or maintenance reasons until the investigation is complete.

The QIRA is required to provide a preliminary forensic report back to the payment card brand within five business days from the onsite review, and a final report is turned in within ten business days from the completion of the review. During this time, the compromised business may also be contacted by the Secret Service regarding the data security breach.

Steps to Remediation and Proof of PCI Compliance Validation

Following the forensic investigation, a conference call is scheduled between the payment card brand, the issuing and/or acquiring bank and the QIRA to discuss the following:

- Length of intrusion
- Total number of cards compromised
- Security flaws
- Remediation steps
- PCI violations



After the investigation and conference call, the issuing/acquiring bank sends all of the “at risk” account numbers that were used during the time of the suspected data security breach to the payment card brand. The business is also notified of the results of the forensic investigation and has 30 days after this date to validate the company’s PCI compliance and complete all remediation steps. These steps can include:

- Submission of a full remediation plan, including implementation dates, to the payment card brand within five days after receiving the final forensic report
- Containment of the incident and implementation of all security recommendations provided by the QIRA, including passing external vulnerability scans and replacing processing hardware where needed
- Removal of any full-track data, CVV2 and/or PIN blocks (including historical data)
- Validation that full-track data, CVV2 and/or PIN blocks are no longer being stored on the systems
- Validation that credit card payment account numbers (PAN) retained for business purposes are stored using PCI compliant encryption
- Monitoring and confirmation completed by the QIRA that the compromised entity has implemented the action plan
- Providing proof that the business achieves full PCI compliance by adhering to the PCI DSS, PA DSS and if applicable, the PCI PIN security requirements

Failure to complete the PCI compliance validation can result in monthly fines, starting at \$5,000 a month, until validation is accepted by the payment card brands.

Additional Fines, Penalties and Repercussions

After the final forensic investigation and conference call, the payment card brands will fine a compromised entity within three to five months. Visa typically charges a \$5,000 fine to businesses that process less than 1 million transactions a year. MasterCard also charges a fine that varies. Within 180 days after the payment card brands have received information of all the “at risk” account numbers, the consumers’ refunds and chargebacks are processed. This has a direct impact on the account owner and the costs associated with these chargebacks will be passed directly to the business from the issuing and/or acquiring banks. The average cost per card stolen ranges anywhere from \$200 - \$1,000 per card.

Once a business has experienced a data security breach, they may also be moved up to Level 1 status for PCI compliance. This means that the business must pass quarterly scans of their external networks by an Approved Scan Vendor (ASV), engage a Qualified Security Assessor (QSA) the following year for PCI compliance validation, and complete an annual Report on Compliance (ROC) and an Attestation of Compliance Form.

In addition to the substantial financial burden, the business can also suffer from damage to its brand reputation and loss of customer loyalty. A data security breach can occur at any time if the proper processes and technology are not put in place. Over 50% of businesses that have been compromised do not survive a data security breach or have a serious disruptive change to its business operations. Many business owners do not believe that a data security breach could happen to them. However, all it takes is one insecure opening to a restaurant provided by out-dated anti-virus, an un-patched operating system, an open firewall or an insecure remote access tool to cause a business to become a victim of a data security breach.