Best Practices for Lodging Merchants to Protect Cardholder Data

The MasterCard Fraud Investigations team has been analyzing incidents of organized hacking groups targeting hotel chains in the U.S., Canada, and Europe regions. These hackers appear to be accessing hotel network systems and possibly compromising cardholder data in storage as well as cardholder data that moves through the authorization process.

Hackers are using specialized malicious software tools (malware) to locate magnetic stripe data stored within active file directories. Hackers are also using such malware to monitor point-of-sale (POS) processes to capture magnetic stripe data from system memory. Password cracking tools, backdoor remote access tools, and malicious tools that hide hacker activity are also used by hackers in hotel-related compromise events.

Identified Security Vulnerabilities

Common security vulnerabilities that hackers exploit in these account data compromise events include, but are not limited to:

- Insecure use of remote access applications (for example, the use of weak or common passwords to access multiple hotel locations)
- Flat network topology, where multiple hotel locations are networked within a single domain and where the payment card processing segment is located within the same segment as corporate systems
- Insecure usage of Internet Web-browsing applications on POS terminals, which can result in the downloading of malware
- Inconsistent usage of anti-virus software
- Usage of non-Payment Application Best Practices (PABP)-validated POS systems that store magnetic stripe data in active directory files
- Failure to restrict outbound access from hotel locations to the Internet via firewall rules

Best Practices for Protecting Cardholder Data

Acquirers and their lodging merchants should review the *Payment Card Industry Data Security Standard* (PCI DSS) requirements and consider the following best practice security measures to help prevent intrusion by hackers.

Use Strong Passwords (Combination of Alphanumeric and Special Characters) That are At Least Eight Characters in Length and Contain No Dictionary Words

Strong passwords are the first line of defense for a network, because hackers will often first try to find accounts with weak or non-existent passwords. Weak passwords are typically short, simple to guess, or are not updated frequently. Strong passwords can be enforced and maintained by enabling the password and account security features that are found on operating systems, networks, databases, and other platforms.

Employ Remote Access Using a Two-factor Authentication Protocol

Two-factor authentication requires two forms of user verification for higher-risk access points, such as those originating from outside of a network. For additional security, entities should also consider using two-factor authentication when accessing networks of higher security from networks of lower security (for example, from a corporate desktop with lower security to a production server or database with high security). In addition to employing a two-factor authentication protocol, entities should also employ remote access on an as-needed basis and log all sessions.

Upgrade POS Systems to PABP-validated Versions and Securely Delete Any Stored Cardholder Data

Insecure applications are one of the leading causes for account data compromise events. Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading the compromises of full magnetic stripe data, card validation codes and values (such as Card Authentication Value 2 [CAV 2], Card Identification [CID] number, Card Validation Code 2 [CVC2], and Card Verification Value 2 [CVV2]), personal identification numbers (PINs), and PIN blocks.

Members use payment applications to store, process, and transmit cardholder data. Since members must be PCI DSS-compliant, members need to be aware that their payment applications should facilitate PCI DSS compliance, rather than prevent it. However, a number of payment applications may prevent compliance if they:

- Store magnetic stripe data in an entity's network after authorization
- Require entities to disable other features required by the PCI DSS, such as anti-virus software or firewalls, for the payment applications to work properly

- Allow vendors to use insecure application connection methods to provide support for members

Address Web Browsing on POS Terminals Through Proper Filtering of Potentially Dangerous Web Sites

Malware can enter a network via many business-approved activities including employee e-mail messages, Internet usage, mobile computing devices, and removable storage devices. Once these malware programs—which can include viruses, worms, and Trojans—enter a network, they can quickly exploit system vulnerabilities and provide hackers with access to payment card data and other personal information.

Install Anti-virus Measures on All Servers and Terminals, and Routinely Monitor Anti-virus Logs

Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. New forms of malware can spread quickly—sometimes within hours of being introduced among the hacking community—so entities must regularly update anti-virus software to mitigate new streams of attacks.

Configure Firewalls to Restrict Outbound Internet Access, and Segment Payment Card Processing from Corporate Systems via Firewall

All systems must be protected from unauthorized access from untrusted networks, such as Internet access via desktop browsers, business-to-business connections, wireless networks, or other sources. Often seemingly insignificant paths to and from untrusted networks can provide a clear pathway to a key system. Firewalls provide a protection mechanism for any computer network, because they prevent hackers from:

- Accessing an entity's networks via an unauthorized Internet Protocol (IP) address, or

- Using protocols and ports in an unauthorized manner, such as sending internal data from an entity's server to an untrusted server.

All firewalls should include a rule that denies all unnecessary inbound and outbound traffic. This rule will help prevent inadvertent "holes" from allowing unintended and potentially harmful traffic in or out of an entity's network.

Segment the Network's Cardholder Data Environment from the Rest of the Entity's Corporate Network

Without adequate network segmentation, an entity's entire network and its database resources can be targeted by hackers. Such hackers can gain access to any point in the network via a structured query language (SQL) injection or other method of remote

access via third-party connections. Segmentation can be achieved by using internal firewalls, routers with strong access control lists, and other technology that restricts access to a particular segment of a network.

If you have any questions regarding this bulletin, please contact your Relationship Manager.

UMS Banking℠
Payment Processing Services