

Visa Data Security Bulletin

Payment System Security Best Practices For Franchises

August 4, 2009

Franchise businesses are increasingly becoming targets of Internet attacks resulting in cardholder data compromises. Hackers continue to exploit weaknesses in vulnerable payment card processing systems with the intention of stealing sensitive customer account information, such as payment card account numbers. In particular, hackers are targeting the full contents of the magnetic stripe (“track data”), Card Verification Value 2 (“CVV2”), a three-digit code imprinted on the back of a Visa card and Personal Identification Numbers (“PIN”). In an effort to promote data security within the franchise sector, Visa has developed security best practices franchisors should employ to help franchisees meet their obligation to comply with the Payment Card Industry Data Security Standard (“PCI DSS”).

Minimize Data Compromises in the Franchise Sector

Visa has developed security best practices that franchisors can utilize to help educate and promote data security within their franchise communities. The strategy is comprised of the following best practice areas: 1) Payment Application Security; 2) Network Security; 3) Remote Management Application Security; 4) Franchisee Contractual Agreements; and 5) Communication and Training. Implementing these security practices will help franchise businesses and their franchisees protect their brands and mitigate their risk of experiencing a security breach and data compromise.

1. Adopt Secure Payment Applications

It is critical that franchisors and franchisees use secure payment applications and do not utilize payment applications known to retain prohibited payment card data or have other inherent security weaknesses. The PCI DSS prohibits the storage of magnetic-stripe, CVV2 or PIN data. Often payment applications lead to the storage of prohibited data post-authorization without the merchant’s knowledge. Hackers intentionally target merchants using these vulnerable payment applications in an attempt to steal sensitive account information. To promote the use of secure applications franchisors should implement the following security best practices:

- Vet current Point of Sale (“POS”) applications with the PCI SSC’s list of validated payment applications. Merchants are encouraged to utilize payment applications that have been validated against the Payment Application Data Security Standard (PA-DSS). This information is available at www.pcisecuritystandards.org/security_standards/vpa.

- Confer with payment application vendors (or resellers / integrators) to ensure their software does not store prohibited data (e.g., magnetic-stripe data, CVV / CVV2 or PIN data).
- Partner with your merchant acquiring bank to obtain a list of vulnerable payment applications. As Visa identifies payment applications that may retain prohibited data, Visa shares this information with acquirers. If payment application deficiencies are identified, franchisors should require that franchisees immediately upgrade to a compliant version. This may be accomplished by implementing an updated application version or patch made available by the vendor or selecting an alternate PA-DSS-validated application. ***In addition to upgrading the application, any historical storage of prohibited data must be securely wiped from all systems immediately.*** A secure wipe utility should be obtained from the application vendor or a third-party vendor.

2. Enforce Network Security

Insecure networks accessible via the Internet are prime candidates for Internet attacks. Factors such as likelihood of sensitive data retention, transaction volume and brand recognition also make franchise networks attractive targets for compromise. To help mitigate the risk of network intrusions originating from the internet franchisors should implement appropriate POS perimeter controls and network security guidelines as prescribed by the PCI DSS. Franchisors should consider the following security practices:

- Mandate franchisees with IP based POS systems and / or broadband connection to install and maintain a stateful hardware firewall at all times. Underscore the consequence of disabling a firewall such as increased likelihood of internet attacks and potential system compromise as well as possible system failure.
- Require franchisees to enable firewall logging and maintain firewall logs for 60 days. These audit trails assist with reconstructing system events, help identify suspicious network activity and are instrumental in facilitating forensic investigations.
- Implement strong access controls. Access controls will help restrict inbound and outbound traffic on known ports to only traffic necessary for the cardholder data environment.

3. Secure Remote Management Applications

Remote Management Applications (“RMAs”) are popular distribution channels amongst many franchise businesses. The ease of use and management across the franchisee platform can serve as an integral part of a franchise business. Many franchisors utilize corporate RMAs throughout their franchise community to disseminate business downloads, conduct sales polls or survey inventory. In addition, select franchisees may establish their own remote management accounts and through these accounts grant vendors remote access to facilitate servicing of the POS system. Consequently, if improperly configured the RMA creates a potential attack vector for hackers to exploit, leaving franchisees vulnerable to data compromise. To secure remote access consider implementing the following:

- Change vendor supplied default settings. Off the shelf RMAs are often packaged from vendors with default or blank passwords. The first step in securing the RMA should be to change the vendor-supplied default settings. By creating unique user IDs and complex passwords (preferably unique to each franchise location) franchisors that use corporate RMA accounts can reduce the risk of data compromise and help facilitate franchisee compliance with the PCI DSS. Franchisees that own and manage a separate account can also benefit from this practice.
- Configure the RMA to allow connections only from specific (known) IP / MAC addresses or configure the system so remote users must establish a Virtual Private Network (“VPN”) connection via a firewall before access is granted.
- Turn on the franchisee’s modem only when needed for downloads from the franchisor or payment application vendor and turn off the modem immediately after downloads are complete. If the franchise business requires the modem configuration in the “always-on” mode, the franchisee and franchisor should consult with the RMA vendor on secure configuration setting for “always-on” mode connections.

4. Amend Franchise Contractual Agreements

Franchisors and franchisees are bound by the terms and conditions of their franchise agreements. As agreements are often renewed between three and five years and are subject to change, during the renewal period franchisors have an opportunity to amend franchisee contracts to include data security policies.

By incorporating data security into the agreements, franchisors can incent franchisees to comply with the PCI DSS which reduces risk of data compromise and helps preserve the integrity of the franchise brand. Franchisors should consider reviewing and amending franchise contracts to include the PCI DSS fundamental security practices, which can be found at www.visa-asia.com/secured.

5. Expand Franchisee Communication and Training

Many franchisors offer both new and ongoing franchisee training programs. Franchisors should consider expanding their training programs to include more robust data security awareness training for franchisees. Consider implementing the following as a part of the franchisor training strategy:

- Create or refine Standing Operating Procedures (“SOP”s). Many franchise businesses maintain operational policy through SOPs to provide operational directives to franchise businesses. Franchisors should amend these procedures to include cardholder data security practices as well as an incident response plan. These response plans should instruct franchisees on the steps required to report and contain a security breach or data compromise. To ensure the plan addresses specific industry mandates such as, immediately notifying merchant acquiring banks and Visa of the event, please visit www.visa-asia.com/secured and review Visa’s “What to do if Compromised” document.
- Direct franchisees to references that will provide practical security guidance. The Visa Account Information Security Program (AIS) web site (www.visa-asia.com/secured) contains an array of security and compliance information, including security bulletins highlighting compromise trends.
- Use a secure automated communication channel, such as a corporate intranet, to distribute timely information such as announcements regarding payment applications used by franchises, data security alerts and training opportunities.
- Direct franchisees to attend data security training and education. Visa conducts webinars to cover key security topics in addition to more detailed security training seminars. Franchisees should partner with their merchant acquiring banks to identify upcoming training events and registration requirements.

For more information or questions regarding the information in this bulletin, please visit www.visa-asia.com/secured or e-mail vpssais@visa.com.