New Year's Resolution . . . Secure Technology

Make your New Year's resolution to reinvest in your business and ensure that you leverage secure technology practices and solutions to protect your business and customer data.

The Payment Card Industry Security Standards Council (PCI SSC), responsible for managing the payment card industry security standards, has published Version 3.0 of the Payment Card Industry Data Security Standard (PCI DSS). Effective 1 January 2015, merchants must validate compliance with PCI DSS version 3.0. The changes in version 3.0 are intended to ease implementation by providing additional flexibility on implementation methods and increases focus on education, awareness and the idea of security as a shared responsibility. Leveraging secure technology in conjunction with PCI DSS v3.0 creates a holistic and robust security plan that aids in securing payment card environments.

Over 95 percent of the world's ATMs are running on XP

Upgrade from Windows XP

Windows XP was removed from Microsoft's list of supported operating systems on 8 April 2014. Announced in 2007, this end of support means Microsoft will no longer release any XP software updates, automatic fixes or service packs. Support for Windows XP Embedded systems expires on 12 January 2016. However, Microsoft reconfirmed they will continue to update the anti-malware engine and signatures through 14 July 2015. Introduced in 2001, XP was the most widely used operating system up until August 2012. As of February 2014, Windows XP still resides on roughly 30% of personal computers worldwide.

Today, many Point-of-Sale (POS) payment applications were programmed to reside on personal computers running XP. Windows XP is already a highly vulnerable platform based on its longevity and its overall architecture. Modern operating systems like Windows 7 and 8 have more sophisticated security features built in, making them less of a target to hackers, who would rather exploit vulnerabilities in older unpatched systems versus developing exploits only to have them undone by a monthly security patch. Anyone using Windows XP, whether it is for personal computing or business operations, should upgrade to a newer and more secure operating system. Additionally, the retirement of XP will impact another business sector – Automated Teller Machines (ATM) owners and deployers. Over 95 percent of the world's ATMs are running XP and migration or upgrading to newer operating systems and hardware has been slow in the industry, leaving thousands of machines to run on the outdated software.

For More Information

Visit visa.com/merchants to learn more fraud prevention tips and resources to help keep your business safe and secure.

EMV chip terminals

EMV chip technology utilizes a computer chip to securely store the card data that currently resides on the magnetic stripe. The chip cards are nearly impossible to counterfeit, and travel will be more convenient in the 130+ countries where chip cards are already accepted.

Prioritize deployment of chip-enabled, dual-interface terminals

- Deploy chip-enabled, dual-interface terminals that support contact chip, Visa payWave and magnetic-stripe interfaces.
  - Merchants that deploy dual-interface terminals are preparing their point-of-sale (POS) environments for mobile payments and other emerging payment technologies.
- Prioritize deployment of chip-enabled, dual-interface terminals by using a targeted approach.
  - Prioritizing the deployment of chip-enabled devices helps minimize potential declines and protects against counterfeit fraud. For example, larger retailers with multiple locations might first deploy in locations with high international acceptance, high overall volume or high counterfeit fraud concentrations.

Tokenization

Payment tokenization is the process of replacing the traditional payment card account number with a unique digital token or digital account number for use in online and mobile transactions. Tokens can be restricted to transactions with a specific mobile device, merchant, or transaction type. The tokenization process is designed to happen in the background in a way that is seamless to the consumer.

Removing sensitive account information provides a more secure way for the industry to enable online and mobile payments

A payment token replaces a primary card account number (PAN), and can be processed by all participants in the payments ecosystem. Payment tokens map back to the underlying account, providing the account issuer with the full transaction details.

Tokens help to simplify the purchasing experience for consumers by eliminating the need to enter and re-enter the account number when shopping on a smart phone, tablet or PC. Tokens or digital account numbers can also help prevent fraud in ecommerce and m-commerce transactions by removing sensitive card account information from the payment process. Finally, merchants and digital payment providers can utilize payment tokens in place of payment account numbers, further helping to enhance payment security.

EMVCo LLC manages an industry standard for tokenization that allows for the traditional 16-digit primary account number (PAN) to be replaced with a digital "token" for online purchases and transactions initiated with mobile devices. Removing sensitive account information provides a more secure way for the industry to enable online and mobile payments.

P2PE technology provides an added layer of protection against the threat of data breaches

P2PE

Point-to-point encryption (P2PE) technology helps merchants and acquirers protect payment card data within their systems by encrypting sensitive cardholder information. Because the card data can only be accessed, or unscrambled, with decryption keys held in a secure environment, cardholder information is protected within the payment processing environment.

This solution is part of Visa's broader authentication strategy which aims to improve payment industry security by eliminating account data from the payment environment whenever possible, protecting sensitive information wherever it is stored, processed or transmitted, and devaluing stolen account information through dynamic authentication solutions such as EMV chip technology. P2PE technology is complementary to EMV chip technology, by providing an added layer of protection against the threat of data breaches, especially as the industry works to reach critical mass in the adoption of chip terminals and chip cards to benefit from EMV's defense against counterfeit fraud.

A point-to-point encryption solution should address several key concerns:

- **Minimal impact to payment processing systems.** Solutions should offer a "format preserving" option, enabling merchants to integrate point-to-point encryption using a 16-digit encrypted value that works with their current systems.
- **Consistent, open encryption standard.** Current standards include Triple Data Encryption Standard (TDES) and Derived Unique Key per Transaction (DUKPT) key management that is used to encrypt PINs today. A solution supporting these standards provides a consistent framework for managing keys and minimizes the impact of merchant system updates.
- **Multi-zone encryption.** The solution should allow for encryption and decryption in multiple zones, providing merchants, gateways and acquirers flexibility in how to deploy encryption within their unique environments. Multi-zone encryption can facilitate routing to multiple endpoints, if the merchant is using multiple processors, consistent with how PIN encryption is managed today.

Consider outsourcing to a PCI DSS validated service provider

Outsourcing ECommerce Payment Operations

For eCommerce merchants, securing the web server is critical. Hosting a site on your own requires significant data security expertise, e.g., professionally trained security and computer forensic professionals. Consider outsourcing to a PCI DSS validated service provider if you don't have appropriate resources.