**Media Contacts**

| |
|---|
| Laura K. Johnson, Ella Nevill |
| PCI Security Standards Council |
| +1-781-876-6250 |
| press@pcisecuritystandards.org |
| Twitter @PCISSC |

PCI Security Standards Council

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

# PCI SECURITY STANDARDS COUNCIL PUBLISHES ATM SECURITY GUIDELINES

*- Best practices to help prevent card data compromise at ATMs -*

**WAKEFIELD**, **Mass**., January 30, 2013— Today the PCI Security Standards Council (PCI SSC), an open, global forum for the development of payment card security standards, published best practices for addressing ATM Security. The *ATM Security Guidelines Information Supplement* was developed with feedback from the PCI community and provides guidance to ATM manufacturers on security steps they can implement in the development of ATMs to help prevent card data compromise at ATMs.

According to findings from the ATM Industry Association's (ATMIA) 2012 ATM Global fraud survey, skimming remains the top global threat to ATMs, with different kinds of brute force attacks continuing unabated. PIN and account data present in ATMs has become a growing target for criminals who use this stolen information to produce counterfeit cards for fraudulent transactions, primarily ATM cash withdrawals.

In response to this growing security concern, the PCI Council worked in conjunction with a number of other industry groups to develop compromise-prevention best practices that stakeholders can leverage in their ATM security efforts. An initial draft of the information supplement was shared with the PCI community in September of 2012, allowing input from those involved in ATM manufacturing and deployment to be incorporated into the final document.

“Skimming and other types of attacks on ATMs continue to be top of mind for our constituents,” said Bob Russo, general manager, PCI Security Standards Council. “There are already some excellent resources out there that help with various pieces of ATM security. What this guidance does is pull together these different best practices into one comprehensive set, which is what our stakeholders have been asking for.”

—more—

The *ATM Security Guidelines Information Supplement* is based on existing standards from a number of industries, including IT, security, payment card and ATM, that address various aspects of ATM security.  The guidance document provides an introduction to ATM security and outlines best practices around the following key areas and objectives:

- Integration of hardware components to avert magnetic-stripe and other account data compromise and PIN stealing
- Security of basic software to avert magnetic-stripe skimming and PIN stealing
- Device management/operation to ensure adequate management of: ATM during manufacturing, ATM in storage of deployed ATM estates and ATM's individual security configuration
- ATM application management to address security aspects of the ATM application.

ATM manufacturers, hardware and software integrators, and deployers of ATMs can use this guidance to aid in the secure development, deployment and maintenance of ATMs. As with all PCI guidance documents the *ATM Security Guidelines Information Supplement* does not replace or supersede the PCI Standards, nor is it to be used as a set of security requirements for the formal certification of ATMs. The PTS POI security requirements provide for the testing and approval of encrypting PIN pads and secure readers used in ATMS for handling PIN and account data, and organizations should continue to use this standard to address these components of ATM security.

The *ATM Security Guidelines Information Supplement* is available in the documents library on the PCI Council website: https://www.pcisecuritystandards.org/security_standards/documents.php.

For additional information, merchants concerned with ATM security should reference *Skimming Prevention: Best Practices for Merchants*, also available on the PCI SSC website.

## About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: http://pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linkedin.com/company/pci-security-standards-council
Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###