Visa Business News

Risk Management | Data Security April 22, 2009

Update on Visa's Compliance Policy to Facilitate Triple Data Encryption Standard Usage

To ensure the highest possible PIN security standards in the electronic payments industry, in 2005, Visa announced a global mandate for Triple Data Encryption Standard (TDES) usage and established July 1, 2010, as the date for global compliance. This mandate requires that all cardholder PINs be TDES protected from the point of transaction to the issuer.

Visa transitioned to TDES because global industry standards bodies (e.g., International Organization for Standardization) no longer recognized the older single-DES (SDES) algorithm for the protection of PINs. Visa's TDES usage mandate is part of a PIN Security and Key Management compliance program that includes other PIN Entry Device (PED) testing mandates focusing on the physical and logical security and TDES capabilities of all devices that accept and process PINs. These mandates were enacted to ensure that Visa, Plus and Interlink payments continue to be the industry's most trusted and secure way to conduct commerce. The substantial progress of TDES implementations made by clients globally is helping to ensure that all payment system participants are protected from increasingly sophisticated threats.

In the U.S., Visa required that all VisaNet and Visa Debit Processing Service endpoints and ATMs use TDES to protect PINs by December 31, 2007. With these major milestones reached, the final U.S. acceptance channel that must achieve TDES compliance is at the point of sale (POS).

Updated Enforcement Policy for POS TDES Usage

Visa will maintain the July 1, 2010, global TDES usage mandate. The enforcement policy for TDES usage will apply separately to each of the following stakeholder categories:

POS TDES Usage—Excluding U.S. Automated Fuel Dispensers (AFDs) at Petroleum Merchants

- **October 1, 2009**—Acquirers must submit to Visa a summary TDES compliance status report and plan to achieve full compliance for sponsored attended POS activity.
- **August 1, 2012**—Acquirers may be assessed fines for sponsoring any non-TDES compliant merchants or agents.

U.S. Petroleum Merchants—TDES Usage

- **October 1, 2009**—Acquirers must submit to Visa a summary TDES compliance status report and plan to achieve full compliance for sponsored

AFD activity.

- **July 1, 2010**—Acquirers may be assessed fines for merchants that are not using at least SDES Derived Unique Key per Transaction (DUKPT) **or** TDES.

- Inside petroleum sales (non-AFD) will be managed under the POS category policy.

U.S. Petroleum Merchants—Encrypting PIN Pad (EPP) Usage

- **January 1, 2009**—Acquirers may be assessed fines for newly deployed AFDs without TDES-capable Payment Card Industry (PCI)-approved EPPs.

- **October 1, 2009**—Acquirers must submit a summary AFD EPP attestation for newly deployed AFDs at sponsored merchants.

This enforcement policy is based on the current risk environment that exists for cardholder PINs accepted at both attended and unattended POS PEDs. Visa will inform clients of any future changes to this policy based on further analysis of exploited vulnerabilities, emerging risks and threats to the payment system.

To protect all payment system participants and ensure continued TDES adoption, clients must develop implementation plans for full TDES compliance. By October 1, 2009, clients must provide to Visa (1) summary TDES compliance status reports and (2) plans to achieve full compliance for all sponsored POS activity. Visa will provide additional guidance to clients on TDES compliance reporting requirements.

In the event of a PIN compromise, acquirers will continue to be subject to Account Data Compromise Recovery, Data Compromise Recovery Solution, or similar program liability (in addition to potential fines) if the entity is found to be non-compliant with the *Payment Card Industry PIN Security Requirements* including *any* use of SDES past July 1, 2010.

To assist clients and merchants with questions regarding AFDs and Visa PED testing requirements, please refer to *Visa's General PED FAQ*, located at www.visa.com/pin.

Secure TDES Migration Recommendations for POS

Clients are encouraged to transition to TDES usage as quickly as possible to provide the highest level of protection for cardholder PINs. To securely migrate to TDES, follow these recommendations:

- Develop detailed plans to migrate to TDES with at least double-length keys.

- In the migration plan, include the conversion of all single-DES DUKPT implementations to TDES DUKPT. When converting from single-DES DUKPT to TDES DUKPT, ensure that new Base Derivation Key components are securely generated.

- Contact POS PED vendors, processors and Encryption and Support Organizations (ESOs) to establish achievable conversion plan milestones for all organizations.

- Evaluate all encryption zones where PIN translations occur to ensure that each zone in which the PIN travels is TDES encrypted from the point of entry all the way to the issuer. This includes any acquirer zone between a PED and a Host

Security Module (HSM) where PIN translations occur.

- Ensure that all POS PEDs use encryption keys unique to that device to process PINs.

- Inspect current equipment inventories (e.g., PEDs, key loading/injection devices and HSMs) to determine 1) which equipment currently supports TDES (with at least double-length keys) and 2) which equipment needs to be upgraded or replaced.

- Ensure that POS PED inventories and new equipment purchases are in compliance with PCI PED testing requirements. PCI-approved PEDs are listed on www.pcisecuritystandards.org/pin. *Visa's General PED FAQ* is located at www.visa.com/pin.

- Contact your processors and POS ESOs to ensure that these entities support TDES-compliant key management controls.

- Target known compromised POS PEDs for replacement first. Known compromised POS PEDs were published in a November 2007 *Data Security Alert* posted on www.visa.com/cisp.

- All attended POS PEDs that have never been successfully lab evaluated and pre-PCI or PCI-approved must be removed from production globally by July 1, 2010. All payment system participants must determine whether any attended vendor-attested POS PEDs are in use; if so, these PEDs must be retired. PEDs in use past July 1, 2010, must be on the current approved list located at www.pcisecuritystandards.org/pin or on the expired approval list located at www.visa.com/pin.

- Ensure full compliance with the *PCI PIN Security Requirements*.

Related Documents

Additional information may be found in the following Visa publications and websites. In addition, Visa is offering ongoing PIN Security and Key Management Trainings throughout 2009. For more information on these workshops, e-mail pinusa@visa.com.

Web Resources:

- Visit www.visa.com/pin to locate these resources:
  - *Visa's General PED FAQ*
  - *Visa PIN Security Tools and Best Practices for Merchants* brochure
- Visit www.pcisecuritystandards.org/pin to locate these resources:
  - Listing of PCI-approved PEDs and other PCI PED testing program information
  - *Payment Card Industry POS* and *EPP PIN Entry Device Security Requirements* manuals
- Visit www.visa.com/pinsecurity to locate these resources:
  - *Payment Card Industry PIN Security Requirements* manual (or visit the "PIN Security" section of Visa Online

For More Information

Contact pinusa@visa.com