VISA PIN SECURITY BULLETIN **2 March 2017**

Visa's U.S. AFD Compliance Policy to Facilitate Triple Data Encryption Standard (TDES) / AES Usage by 1 October 2020

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 and all non-AFD POS achieved TDES compliance by August 1, 2012. With these major milestones reached, the final U.S. acceptance channel that must achieve TDES compliance is at the AFD (POS).

Updated Enforcement Policy for U.S. AFD TDES Usage

Visa will maintain the July 1, 2010, global TDES usage mandate. The enforcement policy for TDES usage at US AFDs has been updated with an end of life sunset date for any remaining SDES usage.

US Petroleum Merchants—TDES Usage

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.

NEW: **Effective October 31, 2020**— SDES Derived Unique Key per Transaction (DUKPT) is no longer an acceptable level of protection for PIN transactions, even in a DUKPT implementation. U.S. AFDs must adopt, at a minimum, TDES with at least double-length keys or AES. Acquirers may be assessed fines for AFD merchants that are not using either TDES or AES for PIN encipherment.

US 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.

This policy is based on the current risk environment that exists for cardholder PINs accepted at AFDs.. 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.

In the event of a PIN compromise, acquirers will continue to be subject to Global Compromised Account Recovery, or similar program liability (in addition to potential fines) if the entity is found to be non-compliant.

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

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

In the migration plan, include the conversion of all single-DES DUKPT implementations to TDES DUKPT or AES. 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) or AES and 2) which equipment needs to be upgraded or replaced.

Ensure that POS PED inventories and new equipment purchases are in compliance with Visa PED Requirements and are PCI-approved devices that are listed on https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices .

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

Target known compromised POS PEDs and expired devices for replacement first.

For More Information

Contact pin@visa.com