



U.S. Point-of-Sale TDES Frequently Asked Questions *Updated August 2009*

On April 22, 2009, Visa published a *Visa Business News* article entitled “*Update on Visa’s Compliance Policy to Facilitate Triple Data Encryption Standard Usage.*” This article is available on www.visa.com/cisp. Visa developed the following Frequently Asked Questions (FAQs) to clarify Visa’s Triple Data Encryption Standard (TDES) compliance policy in the US. These FAQs are based on the April 22, 2009 article and on Visa-specific requirements to comply with the following Payment Card Industry (PCI) standards:

- *PCI PIN Security Requirements*
- *PCI POS PIN-Entry Device Security Requirements**
- *PCI Encrypting PIN Pad Security Requirements**

*In addition to these FAQs, we encourage clients to review the *Visa General PED Frequently Asked Questions*, available at www.visa.com/pin.

For questions regarding Visa’s compliance program requirements for the *PCI Data Security Standard* and *PCI Payment Application–Data Security Standard* please refer to www.visa.com/cisp.

FAQs

General Questions

1. Does Interlink continue to be a preferred PIN network among issuers and merchants/acquirers?

A: Yes, according to ATM & Debit News' 2009 EFT Databook (10/23/08), Interlink is the "top PIN-based POS network in the United States", and Interlink is accepted virtually everywhere PIN pads are present. Interlink is a convenient way for cardholders to pay at PIN-enabled merchant locations throughout the U.S.

2. Why is Visa/Interlink the only Brand to mandate the use of TDES in the Point of Sale (POS) environment?

A: The confidentiality of cardholder PINs accepted and processed at POS PIN Encryption Devices (PEDs) and ATMs depends on all payment system participants fully complying with the PCI standards identified above. These PCI standards are based in part on standards, created by ANSI, ISO and other standards bodies, which have identified a need to migrate from Single Data Encryption Standard (SDES) encryption based on the Data Encryption Algorithm using a single-length key to TDES encryption based on the Triple Data Encryption Algorithm (Triple-DEA) using at least a double-length key.

TDES encryption based on the Triple-DEA algorithm and using at least double-length keys is the industry-standard cryptographic process necessary to support secure PIN-based transactions, whether processed online or offline. These requirements reflect a

U.S. Point-of-Sale TDES Frequently Asked Questions *Updated August 2009*

global awareness that DES-based processes using single-length keys are susceptible to compromise.

In the US, the POS is the last acceptance channel to achieve TDES usage. In 2007, per Visa requirements, all ATMs and VisaNet host-to-host connections were migrated to full TDES usage.

3. What liability and fines will Visa assess upon a sponsoring Interlink acquirer if a sponsored merchant is still using SDES after July 1, 2010 and PINs are compromised due to the use of SDES?

A: All Interlink sponsored merchants accepting PIN debit already are required to comply with both the existing Visa-specific requirements and with the *PCI PIN Security Requirements*. However, after July 1, 2010, the liability risk for Interlink sponsoring acquirers of merchants that continue to use SDES will increase. If the use of SDES contributes to a PIN compromise after July 1, 2010, the sponsored merchant's failure to migrate to TDES will factor into Visa's liability and fine analysis with respect to that sponsored merchant. In the event of a PIN compromise, sponsoring Interlink acquirers may be subject to liability or fines under the Account Data Compromise Recovery (ADCR) program, the Data Compromise Recovery Solution (DCRS), or other similar programs if a sponsored merchant fails to comply with the *PCI PIN Security Requirements*—including *any* use of SDES past July 1, 2010. For further information on the above programs, please visit <http://usa.visa.com/merchants/operations/adcr.html>

Table 1:

Status	Failure to use TDES at all attended POS PEDs	Failure to use TDES or SDES DUKPT at all Automated Fuel Dispensers (AFD)	Continued use of SDES at attended POS PEDs or at AFDs
Fines / Liability	Compliance fines may be assessed after August 1, 2012 <i>whether or not there is a PIN compromise.</i>	Compliance fines may be assessed after July 1, 2010 <i>whether or not there is a PIN compromise.</i> In the event of a PIN compromise, the sponsored merchant's failure to migrate to TDES may factor into Visa's liability and fine analysis.	<i>In the event of a PIN compromise attributable to the use of SDES, fines are possible after July 1, 2010 in addition to ADCR and DCRS program liability</i>

U.S. Point-of-Sale TDES Frequently Asked Questions *Updated August 2009*

4. If a sponsored merchant decides to stop accepting Interlink transactions, will it need to convert to TDES?

A: Sponsored merchants should check with their individual PIN debit networks to determine the security requirements of those networks for secure PIN acceptance.

5. The April 22, 2009 *Visa Business News* article states that “Clients are encouraged to transition to TDES usage as quickly as possible to provide the highest level of protection.” Are retailers required to upgrade to TDES for both their attended POS PEDs and their unattended POS PEDs (Automated Fuel Dispensers, or AFDs) by July 1, 2010?

A: Yes, all sponsored merchants accepting PIN debit transactions are required to transition to TDES by July 1, 2010

- Sponsoring Interlink acquirers must ensure that all of their sponsored merchants' attended POS PEDs are using TDES by August 1, 2012 to avoid potential compliance fines.
- Sponsoring Interlink acquirers must ensure that all sponsored merchants' AFDs are implementing TDES by providing Visa the reporting outlined in FAQ number 9 below.

6. If a sponsored merchant is not able to achieve full TDES usage by July 1, 2010, is it required to obtain an extension from Visa or from its sponsoring Interlink acquirer?

A: Sponsored merchants should contact their sponsoring Interlink acquirer for information regarding specific reporting requirements; requests for extensions should not be submitted to Visa. Through the *Visa Business News* article published on April 22, 2009 and referenced above, Visa has allowed sponsored merchants additional time to implement TDES without necessarily incurring compliance fines. This article is available on www.visa.com/cisp and describes the reporting requirements and time frames by which sponsored merchants must achieve full TDES usage.

Automated Fuel Dispenser (AFD) Related Questions

7. Other than the security benefits of TDES usage, what cardholder preference considerations should petroleum retailers consider in making TDES upgrade investments to AFDs?

A: Interlink acceptance at AFDs is a customer convenience that helps maintain customer satisfaction and customer loyalty. Inconveniencing customers by limiting their AFD payment options may decrease sales, or may steer customers to alternative payment methods which are costlier to the retailer.

8. What fines will Visa assess upon a sponsoring Interlink acquirer if a sponsored merchant is not using SDES DUKPT or TDES at all AFDs by July, 1 2010?



U.S. Point-of-Sale TDES Frequently Asked Questions *Updated August 2009*

A: To avoid compliance fines, sponsoring Interlink acquirers must ensure that all of their sponsored merchants are at a minimum using SDES DUKPT and/or TDES (TDES DUKPT or TDES Fixed Key or TDES Master/Session) at all AFDs. Visa is currently reviewing its PIN security compliance fine structure. Fines assessed after July 1, 2010 will follow the fine structure that is in effect at that time.

9. When will Visa begin to assess fines upon sponsoring Interlink acquirers for sponsored petroleum merchants that are not using TDES at all of their AFDs?

A: To protect all payment system participants and ensure continued TDES adoption, sponsored merchants and their sponsoring Interlink acquirers must develop implementation plans for full TDES compliance. By October 1, 2009, all sponsoring Interlink acquirers must provide to Visa a summary TDES compliance status report. Following that date, all sponsoring Interlink acquirers must submit a quarterly update on their sponsored merchants' plan to achieve full compliance for all sponsored POS activity.

The above quarterly summary TDES implementation status plans must also address the sponsored merchant's progress towards implementing TDES at all AFDs, and must indicate a final TDES usage date for all AFDs. Visa intends to announce a TDES usage date for all US AFDs, after which sponsoring Interlink acquirers whose sponsored merchants do not meet this requirement may be subject to fines.

10. Where can a sponsored petroleum merchant determine the approval status of its current AFD equipment?

A: All AFDs fall into three categories: (1) older, vendor-attested AFDs, (2) pre-PCI AFDs, and (3) AFDs containing PCI-approved Encrypting PIN Pads (EPPs). Sponsored merchants must ensure that all AFDs newly deployed after January 1, 2009 contain a TDES-capable, PCI-approved EPP. Visa may assess fines upon sponsoring Interlink acquirers for any sponsored merchants that newly deploy an AFD after January 1, 2009 that does not contain a TDES-capable, PCI-approved EPP. Please refer to www.pcisecuritystandards.org/pin for a listing of PCI-approved EPPs. By October 1, 2009, all sponsoring Interlink acquirers must submit a summary AFD EPP attestation to Visa for all AFDs deployed since January 1, 2009 at their sponsored merchants.

For older AFD solutions, sponsored merchants are encouraged to review the *Visa General PED Frequently Asked Questions* document available on www.visa.com/pin or contact their AFD vendors directly. As noted in that document, the intent of the EPP requirement is not retroactive; however, most legacy AFD installations will require that an EPP be installed to process TDES transactions. Visa intends to announce a TDES usage date for all US AFDs, after which sponsoring Interlink acquirers whose sponsored merchants do not meet this requirement may be subject to fines. Consistent with the April 22, 2009 *Visa Business News* article, the continued operation of AFDs that use SDES DUKPT encryption thus remains permissible in the short term absent a PIN compromise, although Visa may impose fines based on a PIN compromise attributable



U.S. Point-of-Sale TDES Frequently Asked Questions *Updated August 2009*

to the use of SDES rather than TDES, and in such case, Visa may take into account in its liability and fine analysis the sponsored merchant's failure to migrate to TDES.

11. May EPPs that are not TDES-capable be installed after January 1, 2009?

A: Sponsored merchants must ensure that all AFDs newly deployed after January 1, 2009 contain a TDES-capable, PCI-approved EPP. In some cases, non PCI-approved EPP solutions purchased prior to January 1, 2009 may be installed in existing AFDs. Sponsored merchants should review the *Visa General PED Frequently Asked Questions* document, available at www.visa.com/pin, to review the criteria of a newly deployed AFD and should check with their sponsoring Interlink acquirer to determine whether a non-PCI approved EPP solution purchased prior to January 1, 2009 may be installed in an existing AFD.

Attended Point-of-Sale Related Question

12. What fines will Visa assess upon a sponsoring Interlink acquirer if a sponsored merchant is not using TDES at all of its attended POS PEDs after August 1, 2012?

A: Visa is currently reviewing its PIN security compliance fine structure. Fines assessed after August 1, 2012 will follow the fine structure that is in effect at that time.