CHIP ADVISORY #19, OCTOBER 11TH, 2011

Dynamic Authentication" does not mean "DDA"

Summary

On August 9, 2011, Visa announced plans to accelerate chip adoption in the United States. There has been a misconception regarding what Visa means by the term "dynamic authentication" as used in the announcement and subsequent communications. This Chip Advisory corrects and clarifies this misconception.

In short, Visa does not mean to suggest that the United States market adopt chips using Dynamic Data Authentication ("DDA") technology (defined below). While DDA technology is useful in markets that require offline authorization capability, it also adds complexity and cost to the payment system. Since the U.S. already has a ubiquitous, fast and inexpensive online payment system, offline authorization support is not necessary. In many instances Visa can provide an online authorization as fast as a payment terminal can perform an offline authorization.

Visa suggests U.S. financial institutions issue online-only chip cards. Such cards work in virtually all payment terminals globally. For the same reasons, offline authorization capability is unnecessary for merchants and acquirers in the U.S. Supporting offline authorization in an online market such as the U.S. adds cost to the payment terminals and supporting infrastructure without providing merchants with any additional payment utility or fraud protection (see Q/A3 for additional detail).

☒ Issuer

☒ Acquirer

☒ Chip Vendors

☒ Chip Card Vendors

☒ Chip Terminal Vendors

☒ Chip Card Personalization Bureaus

☐ Other

Discussion

What is Dynamic Authentication?

Authentication is the act of validating that something is genuine. This is often done through the use of static data such as a Card Verification Value (CVV) encoded on magnetic stripes. If static data is compromised, then it can no longer be relied upon for authentication. However, authentication systems that rely on dynamic data are less

susceptible to this type of problem since the data to be authenticated changes upon each use. Therefore, stealing a single value would have little or no utility to a fraudster. The technical details of how dynamic authentication systems work are beyond the scope of this document; the key point is that dynamic authentication systems are substantially more secure than static authentication systems.

What is DDA?

DDA is defined in the EMV specifications. It is a specific method for a chip terminal to authenticate a chip card. It is often used for chip transactions that occur in markets that support offline authorizations. While DDA provides strong authentication of the card, it is not needed when the card will be authenticated online since all EMV cards produce dynamic authentication data known as the "cryptogram". This cryptogram is validated by the issuer or its processor in an online transaction and provides authentication just as strong as the authentication provided by DDA. Furthermore, in online environments, the cryptogram is always produced and sent to the network, so performing DDA, in addition to sending the cryptogram, is redundant. As mentioned above, supporting DDA is more expensive and time consuming than supporting an online only solution. Therefore for countries with ubiquitous online authorization capabilities, DDA is unnecessary.

Frequently Asked Questions

FAQs for Merchants/Acquirers

Q1: I'm a merchant that sees many foreign cards. Should I support DDA (or any other form of offline data authentication[1])?
A1: No. Foreign cards will work in terminals that do not support DDA or any other form of offline data authentication.

Q2: Does support of DDA (or any other form of offline data authentication) impact the routing of a transaction?
A2: No. DDA (or any other form of offline data authentication) support has no impact on transaction routing.

Q3: I'm a merchant that has a large number of transactions that cannot go online, e.g., buy onboard. Should I support DDA (or any other form of offline data authentication)?
A3: For the U.S. market, Visa requires that all transactions be authorized online in order to enjoy all protections and benefits of Visa card acceptance. Therefore merchants with a large number of transactions that cannot go online typically perform a delayed authorization request once they are able to go online. Merchants that frequently cannot perform online authorizations *may* wish to support offline data **authentication** *if they also see a high degree of international cards*. Doing so might help such merchants identify counterfeit cards.

[1] Offline data authentication is a process where card data is validated by the merchant terminal. This process is not needed for online transactions since the card data is validated by the network or issuer.

FAQs for Issuers

Q4: As an issuer, do I need to support DDA for my international travelers?
A4: No. DDA is not needed for international traveler cards. Virtually all payment acceptance points worldwide support online-only cards.

Q5: Does support of DDA impact the choice of PIN or signature being used at the POS?
A5: No. PIN transactions in the US today are also conducted online and, hence DDA support has no impact on PIN transactions.

If you have additional questions, please contact technologypartner@visa.com.