Aite PARTNER. ADVISOR. CATALYST.

3-D Secure 2.0: Key Considerations for Merchants

OCTOBER 2018

Prepared for:

NuData Security

mastercard

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

3-D Secure 2.0: Key Considerations for Merchants, commissioned by NuData Security and produced by Aite Group, provides an explanation of the benefits introduced with 3-D Secure (3DS) 2.0 and key considerations for merchants as they determine how to deploy the solution.

Key takeaways from the study include the following:

- 3DS 2.0 has the potential to be a key tool in the arsenal of issuers and merchants in the fight against card-not-present (CNP) fraud. This new-and-improved version of the 3DS protocol will provide an enhanced data stream between issuers and merchants to better inform authentication and authorization decisions. The data shared increases from the 15 fields supported by 3DS 1.0 to over 150 data fields in 3DS 2.0. This promises to not only reduce fraud but to also significantly impact the equally harmful false declines.
- The new protocol is mobile-friendly, an important attribute as mobile commerce continues to grow rapidly in countries around the globe.
- Another key enhancement in 3DS 2.0 is the ability for merchants to turn on 3DS in data-only or nonchallenge mode so that they benefit from 3DS in various ways without the risk of a stepped-up authentication prompt to the consumer.
- As merchants contemplate their path to 3DS 2.0 enablement, they should look for a vendor that is well-versed in the nuances of 3DS. The enabling vendor should be able to address whether the transaction is eligible for the liability shift and what type of stepped-up authentication (if any) the merchant should expect from the issuer on the other side of the transaction.
- 3DS is not a silver bullet, and as such, merchants should look for vendors with a broad range of transaction risk capabilities. A range of frictionless risk assessment and authentication capabilities can help the merchant decide whether it wants to invoke 3DS at all, so it's important to look for a vendor that can support this.

INTRODUCTION

It's no secret. As countries around the globe make the move to EMV, the organized crime rings behind financial fraud won't give up their criminal efforts and get a real job. They switch tactics, and CNP fraud is one of the primary areas to which fraud migrates. This presents a challenge for issuers and merchants alike, since an increasing proportion of payment card purchases are migrating to CNP channels.

The approach to mitigating CNP card fraud varies. Many merchants have deployed multiple layered fraud solutions designed to aid detection with minimal transactional friction, while a number of countries have mandated multifactor authentication for CNP transactions. The key challenge rests in how issuers and merchants can balance the need to prevent fraud with the competitive driver of providing easy, user-friendly customer experiences. For issuers and merchants alike, the specter of false declines and the resulting customer dissatisfaction is usually more troubling than potential fraud losses.

3DS 2.0[1] has the potential to be a key tool in the arsenal of issuers and merchants. This new-and-improved version of the 3DS protocol will provide an enhanced data stream between issuers and merchants to better inform authentication and authorization decisions. Such a substantial expansion of the concept requires a fair amount of planning and strategizing, however. This white paper provides insight into the key factors that merchants need to take into consideration as they plan their move to 3DS 2.0.

METHODOLOGY

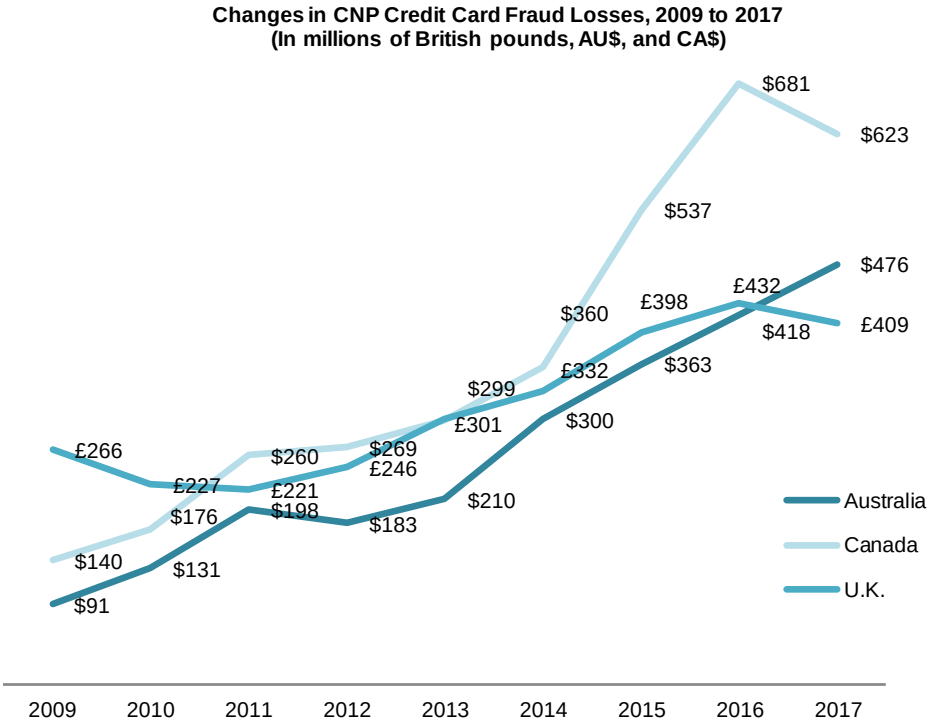
This white paper is informed by Q1 2018 interviews with global payment networks, issuers, merchants, and fraud mitigation vendors as well as ongoing conversations with executives in the space about their current and planned use of 3DS.

1. While officially named EMV 3-D Secure, the widely used industry term for the new protocol is 3-D Secure 2.0, so it will be referred to by this name throughout the report.

THE MARKET

A perfect storm has converged around CNP fraud, driving losses higher globally (Figure 1). As countries around the globe migrate to EMV chip cards, organized crime rings have shifted their focus away from counterfeit cards at the point of sale over to digital channel fraud attacks. The loss data in Figure 1 brings a glimmer of good news: After years of steadily rising CNP fraud losses in the U.K. and Canada, both countries saw a slight decrease in 2017. However, the U.K. numbers aren't quite as rosy as they appear at first glance—the driver of the decrease in overall CNP fraud losses was due to a 13% decrease in mail and telephone order (MOTO) fraud, while e-commerce fraud increased by 8% from 2016 to 2017.[2]

Figure 1: Global CNP Fraud Losses



Source: Canadian Bankers Association, Financial Fraud Action U.K., and Australian Payments Clearing Association

Three key factors are contributing to the increase in CNP fraud:

2. "Fraud the Facts 2018," UK Finance, August 2018, accessed on September 1, 2018, https://www.ukfinance.org.uk/wp-content/uploads/2018/07/Fraud-the-facts-Digital-version-August-2018.pdf.

- **Migration to EMV:** As EMV effectively reduces levels of counterfeit fraud, criminals shift their tactics to new account fraud, account takeover, and CNP fraud.[3]
- **Data breaches:** As a result of the vast number of data breaches that compromise payment card data, login credentials, and personally identifiable information, criminals have a wealth of data at their disposal to use in their fraud attacks.
- **E-commerce growth:** Consumers' buying behaviors are increasingly digital. E-commerce is growing at double-digit rates in most countries (Table A), far eclipsing brick-and-mortar retail growth.[4]

Table A: 2017 Global E-Commerce Growth Rates

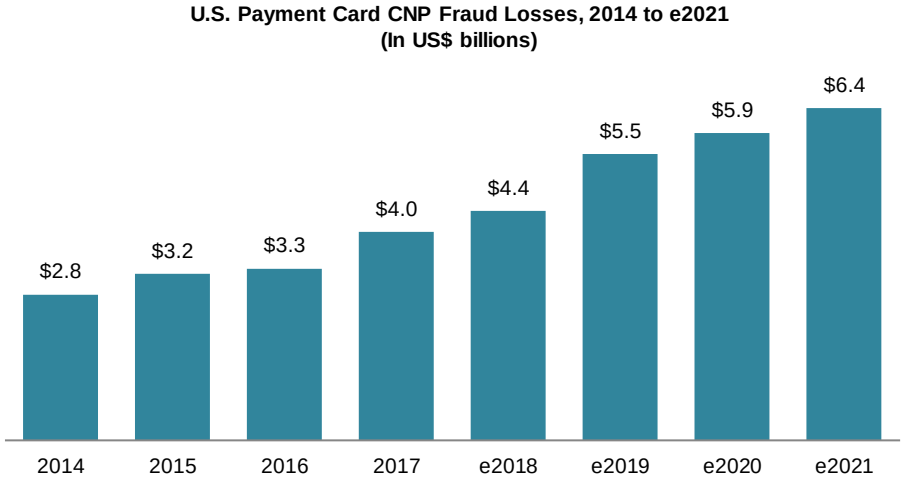
Country	E-commerce growth rate	Country	E-commerce growth rate
Australia	40%	**India**	17%
Turkey	31%	**U.K.**	16%
Mexico	26%	**Japan**	16%
Italy	26%	**Chile**	15%
Spain	25%	**South Korea**	15%
Russia	25%	**Brazil**	14%
Argentina	22%	**Saudi Arabia**	11%
France	21%	**Canada**	9%
Indonesia	20%	**U.S.**	9%
China	20%	**Israel**	8%
Germany	18%		

Source: Ecommerce Europe

The U.S. is no exception to the rising CNP fraud trend, as shown in Figure 2.

3. See Aite Group's report *EMV: Issuance Trajectory and Impact on Account Takeover and CNP*, May 2016.
4. "Ecommerce Europe Global B2C Ecommerce Country Report 2017," Ecommerce Europe, accessed on December 28, 2017, https://www.ecommerce-europe.eu/research/ecommerce-europe-reports.

Figure 2: U.S. CNP Fraud



Source: Aite Group

For many merchants, however, false declines are more troubling than fraud losses. False declines occur when a good customer's transaction is mistakenly declined because of false positives in the issuer's or merchant's fraud screens. In the U.S. market alone, false declines for payment card transactions totaled US$303 billion in 2017. The CNP channels are disproportionately impacted by false declines, with the average decline rate for a CNP transaction hovering around 15% to 20%, versus 2% to 3% for card-present transactions.

3DS 2.0 offers the potential to help issuers address false declines as well as rising CNP fraud. Table B summarizes the market trends that indicate that the time is right for a move to a more robust CNP fraud prevention regime.

Table B: Market Trends and Implications

Market trends	Implications
Rising CNP fraud attacks	Increasing CNP fraud attacks are driving issuers and merchants alike to seek out better means of protecting digital commerce transactions.
Focus on reducing false declines	False declines damage the customer's relationship with both the issuer and the merchant, and they result in potential lost revenue. Issuers and merchants are looking for ways to significantly reduce false declines.

Market trends	Implications
Competitive push for frictionless commerce	Consumers expect e-commerce to be easy and elegant and are willing to take their business elsewhere if the purchasing experience is cumbersome. As a result, merchants favor fraud prevention techniques that do not require consumer participation.

Source: Aite Group

WHAT IS 3DS?

3DS is a standard managed by EMVCo that enables issuers to perform additional risk assessment at the time of an e-commerce transaction and prompt the consumer for additional authentication if the transaction appears to be risky. 3DS is a common communication protocol across the card networks. Each has established its own separately branded program that establishes the rules and incentives for 3DS participation, as illustrated in Table C.

Table C: 3DS Across the Brands

Payment brand	3DS program name
American Express	SafeKey
Discover	ProtectBuy
JCB International	J/Secure
Mastercard	Identity Check (3DS 2.0) SecureCode (3DS 1.0)
Visa	Verified by Visa (VbV)

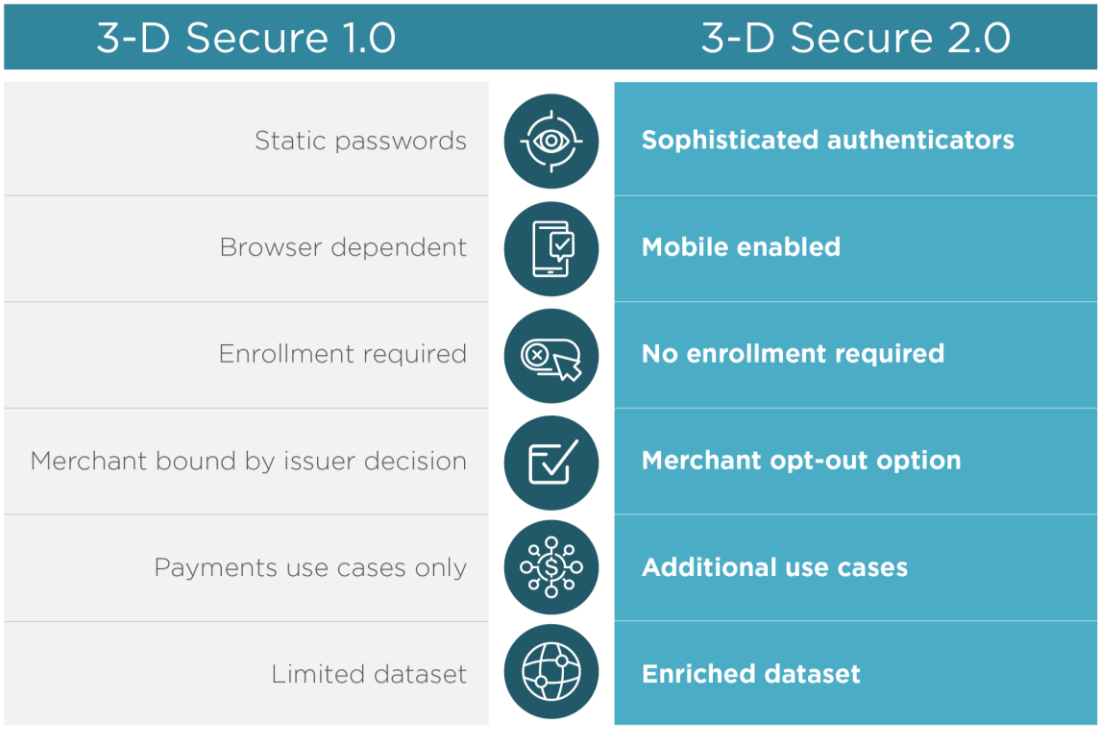
Source: Aite Group

In its initial incarnation, 3DS was viewed by many merchants and issuers as an obstacle to sales rather than as a fraud-prevention solution due to its clunky user experience. The payment networks and enabling vendors made substantial changes to the process over the ensuing years, and the last version of 3DS 1.0 was much improved. One of the most important enhancements was a transition from a binary approach to authentication in which all transactions are subjected to a stepped-up authentication prompt to the option of risk-based authentication. Even so, there were fundamental gaps in the first version of the protocol that could only be addressed by releasing an entirely new version.

EVOLUTION TO 2.0

After a lengthy collaborative process, EMVCo released the 3DS 2.0 specification in October 2016. The key differences between 3DS 1.0 and 3DS 2.0 are summarized in Figure 3 and are further elaborated below.

Figure 3: Differences Between 3DS 1.0 and 3DS 2.0



Source: Aite Group

- **Sophisticated authenticators:** Static passwords are not only ineffective, but they're also not very user-friendly. 3DS 2.0 moves the protocol from static passwords to complex authenticators, such as biometrics and one-time passwords (OTPs).
- **Mobile enabled:** The smartphone had not yet been invented when the first version of 3DS was released. 3DS 2.0 is capable of seamlessly integrating with mobile apps as well as browser-based environments.
- **No enrollment required:** 3DS 2.0 eliminates the active enrollment requirement. Many of the vendors' risk-based authentication access control server solutions had already introduced this enhancement, so it is available to many issuers on 3DS 1.0.2, but going forward it will be formalized within the protocol.
- **Merchant opt-out:** Many merchants would like the ability to turn on 3DS in nonchallenge mode so that they can feed those results into their own risk models and use that to inform their own approve/decline decisions (understanding that they wouldn't benefit from the liability shift). While 3DS 1.0 did not offer this, 3DS 2.0 provides this capability.
- **Additional use cases:** While 3DS 1.0 was architected around the payment transaction, 3DS 2.0 supports additional use cases, such as account verification and token provisioning.

- **Enriched data set:** 3DS 1.0 supports 15 data elements. The 3DS 2.0 data set has significantly expanded with more than 150 data elements, some of which are required and others that are optional. A sample of some of the incremental fields in the 3DS 2.0 data set are found in Table D.[5]

Table D: 3DS 2.0 Data Element Samples

Data element	Required?	Definition
3DS requestor authentication method	Optional	Mechanism used by the cardholder to authenticate to the 3DS requestor Examples include the following: • 01 = No 3DS requestor authentication occurred (i.e., cardholder "logged in" as guest) • 02 = Log in to the cardholder account at the 3DS requestor system using 3DS requestor's own credentials • 03 = Log in to the cardholder account at the 3DS requestor system using federated ID • 04 = Log in to the cardholder account at the 3DS requestor system using FIDO authenticator • 05 = Log in to the cardholder account at the 3DS requestor system using third-party authentication • 06 = Log in to the cardholder account at the 3DS requestor system using FIDO authenticator
Browser IP address	Conditional	IP address of the customer's browser
Browser language	Required	Language used by the customer's browser
Cardholder account age indicator	Optional	Length of time that the cardholder has had the account with the 3DS requestor. The following values are accepted: • 01 = No account (guest checkout) • 02 = Created during this transaction • 03 = Less than 30 days • 04 = 30 to 60 days • 05 = More than 60 days

5. For a comprehensive listing of the 3DS 2.0 data elements, see "Protocol and Core Functions Specification," EMV 3DS, October 2017, accessed September 20, 2018, https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_210_1017.pdf.

Data element	Required?	Definition
Cardholder account change indicator	Optional	Length of time since the cardholder's account information with the 3DS requestor was last changed—including billing or shipping address, new payment account, or new user(s) added
Delivery time frame	Optional	Indicates the merchandise delivery time frame
Gift card amount	Optional	For prepaid or gift card purchase, the purchase amount total of prepaid or gift card(s)
Merchant category code	Required (for payment transactions)	Specific code describing the merchant's type of business, product, or service
Shipping indicator	Optional	Indicates shipping method chosen for the transaction Merchants must choose the shipping indicator code that most reasonably and fairly describes the cardholder's specific transaction, not their general business. Examples include the following: • 01 = Ship to cardholder's billing address • 02 = Ship to another verified address on file with merchant • 03 = Ship to address that is different than the cardholder's billing address • 04 = "Ship to store"/pick up at local store (store address shall be populated in shipping address fields) • 05 = Digital goods (includes online services, electronic gift cards, and redemption codes) • 06 = Travel and event tickets, not shipped • 07 = Other

Source: Aite Group, EMVCo

The enriched data set has the potential to provide a significant performance boost. The CNP decisioning environment for issuers and merchants is akin to two people dividing a box of puzzle pieces and separately trying to put together the puzzle. Merchants have valuable data about the customer's behavior but historically had no way to share those insights to help inform the issuer's authorization and authentication decisions. A customer that has successfully been authenticated in the merchant's mobile app using a strong authenticator, such as a biometric, and who is a long-standing customer of the merchant with no recent account changes presents a low risk of fraud. Conversely, if the customer is new to the merchant and is ordering for pickup at a store that is far from the address on file at the issuer, stepped-up authentication may be warranted. 3DS 2.0 finally provides the mechanism for merchants to share this data with issuers to reduce false declines while better detecting fraud.

LATENCY REDUCTION

Another benefit of additional data elements is the potential reduction in latency. In 3DS 1.0, the protocol enforces two authentication cycles for every transaction, regardless of whether the cardholder is presented with a stepped-up authentication request. As a result, the average transaction time usually exceeds several seconds, which is far beyond many merchants' tolerance for latency. With 3DS 2.0, the expectation is that the enhanced data exchange will facilitate frictionless authentication at least 90% of the time. When frictionless authentication occurs in 3DS 2.0 only one authentication cycle is required, which will significantly reduce the average transaction time.

3DS 2.0 BENEFITS

The benefits of merchants adopting 3DS 2.0 include the following:

- **Liability shift:** The fraud liability for transactions that travel across the 3DS protocol shifts from the merchant to the issuer.
- **Higher authorization rates:** 3DS transactions generally see 10% to 11% higher authorization rates than non-3DS transactions. Mastercard and Visa are providing the opportunity to further boost these rates by enabling visibility to authentication information in the authorization message.
- **Reduced false declines:** The enhanced data exchange promises to help issuers make better authorization decisions, putting a dent in the false decline problem.
- **Regulatory compliance:** In response to rising fraud, many countries either have already or are in the process of mandating multifactor authentication for CNP transactions. 3DS 2.0 provides compliance with the vast majority of these mandates, as described in Table E.

Table E: Multifactor Authentication Mandates

Country/ region	Mandating entities	Description
Australia	Mastercard	All transactions over US$200 require 3DS.
	Visa	Until April 12, 2019: All credit, debit, and reloadable prepaid cards must be enrolled in VbV. A merchant must support VbV if the merchant's fraudulent Visa e-commerce transaction volume is US$25,000 or higher and exceeds 0.25% of the merchant's overall e-commerce transaction volume, or if the merchant's fraudulent Visa e-commerce transaction volume is US$250,000 or higher and exceeds 0.025% of the merchant's overall e-commerce transaction volume. If the merchant exceeds the merchant fraud threshold, it must implement VbV within 120 days of discovery. Acquirers must ensure their merchants use VbV if they exceed the merchant fraud thresholds in any quarter. Effective 13 April 2019: Merchants must process an e-commerce transaction using VbV 3DS 2.0 if it is assigned any of the following merchant category codes (MCCs): 4722 (travel agencies and tour operators), 4816 (computer network/information services), 4829 (wire transfer money orders), 5085 (industrial supplies), 5311 (department stores), 5399 (miscellaneous general merchandise), 5411 (grocery stores and supermarkets), 5661 (shoe stores), 5691 (men's and women's clothing stores), 5699 (miscellaneous apparel and accessory shops), 5722 (household appliance stores), 5732 (electronics stores), 5733 (music stores—musical instruments, pianos, and sheet music), 5734 (computer software stores), 5912 (drug stores and pharmacies), 5943 (stationery stores, office and school supply stores), 5944 (jewelry stores, watches, clocks, and silverware stores), 5999 (miscellaneous and specialty retail stores), 6211 (security brokers/dealers), 7011 (lodging—hotels, motels, resorts, central reservation services), 7832 (motion picture theaters), 7995 (betting, including lottery tickets, casino gaming chips, off-track betting, and wagers at race tracks), 8999 (professional services), or 9402 (postal services—government only). If a merchant is not enrolled in VbV 3DS 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the high-risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Bangladesh	Mastercard	All acquirers and merchants must support 3DS 2.0 by October 2019.
Brazil	Visa	Issuers must ensure that debit and Electron bank identification numbers (BINs) participate in VbV.
Canada	Visa and Mastercard	Issuers must ensure that business and consumer debit BINs participate in 3DS.

Country/ region	Mandating entities	Description
China	Visa	Issuers' VbV program must use dynamic authentication.
Europe	European Commission	The second Payment Services Directive (PSD2) mandates strong customer authentication (SCA) to be implemented for electronic transactions. Payment service providers, which include banks, e-money providers, and payment institutions, must apply SCA for all electronic payments initiated by the payer (such as card payments and credit transfers), unless the payment qualifies as low risk and falls within a set of specified exemptions.
	Mastercard	3DS is required for all online gaming transactions. On a staggered basis from April 2019 to September 2019 (timelines will coincide with the PSD2 Regulatory Technical Standard (RTS) effective dates), Mastercard will require European issuers, acquirers, and merchants to support 3DS 2.0 on e-commerce transactions. In select markets, issuers will also be required to enable biometric authentication on mobile devices that support the technology.
	Visa	Issuers that submit secure e-commerce transactions must support VbV. Acquirers must ensure that all high brand-risk merchants and high brand-risk sponsored merchants process e-commerce transactions using a Visa-approved payment authentication method.
India	Reserve Bank of India	Dual-factor authentication is required for all card transactions above 2,000 rupees.[6] The latter threshold was introduced recently to reduce payment friction and respond to the needs of e-commerce firms, online ticket booking companies, and taxi-hailing apps.
	Mastercard	All acquirers and merchants must support 3DS 2.0 by October 2019.
Japan	Japan Online Game Association	All association members are required to implement 3DS.
Malaysia	Mastercard	All acquirers and merchants must support 3DS 2.0 by October 2019.
New Zealand	Mastercard	All transactions over US$200 require 3DS.

6. "Card Not Present Transactions—Relaxation in Additional Factor of Authentication for Payments up to ₹ 2000/- for Card Network Provided Authentication Solutions," Reserve Bank of India, December 6, 2016, accessed October 17, 2017, https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=10766.

Country/ region	Mandating entities	Description
	Visa	All Visa credit, debit, and reloadable prepaid cards must be enrolled in VbV. Virtual accounts associated with Visa commercial cards are excluded from this requirement. A merchant must support VbV if the merchant's fraudulent Visa e-commerce transaction volume is US$25,000 or higher and exceeds 0.25% of the merchant's overall e-commerce transaction volume, or if the merchant's fraudulent Visa e-commerce transaction volume is US$250,000 or higher and exceeds 0.025% of the merchant's overall e-commerce transaction volume. In addition, e-commerce merchants must use VbV or an equivalent Visa-approved authentication method if the merchant exceeds US$10,000 in Visa transaction volume in any quarter or is assigned one of the following MCCs: 4814 (telecommunication services), 5499 (miscellaneous food stores, convenience stores, and specialty markets), 5732 (electronics stores), 5734 (computer software stores), 5941 (sporting goods stores), 5944 (jewelry stores, watches, clocks, and silverware stores), 5947 (gift, card, novelty, and souvenir shops), 6300 (insurance sales, underwriting, and premiums), 7399 (business service not elsewhere classified), or 9399 (government services not elsewhere classified).
Nigeria	Visa	Nigerian issuers must ensure each cardholder is enrolled in VbV and only authorize domestic e-commerce transactions for which the acquirer has requested VbV authentication, except for transactions processed under the International Airline Program.
	Mastercard	All acquirers and merchants must support 3DS 2.0 by October 2019.
Singapore	Monetary Authority of Singapore (MAS)	All online transactions must be authenticated via a dynamic OTP via 3DS.
South Africa	Payment Association of South Africa	All issuers and e-commerce merchants must support 3DS.
	Mastercard	All acquirers and merchants must support 3DS 2.0 by October 2019.
South Korea	Financial Supervisory Service	Multifactor authentication is required for e-commerce transactions.
Taiwan	Taiwanese government	A government directive set forth a recommendation for 3DS adoption that has been interpreted as a mandate by Taiwanese banks.

Source: Aite Group, Visa, Mastercard

PSD2 STRONG CUSTOMER AUTHENTICATION REQUIREMENT

While 3DS 2.0 is moving in the direction of minimizing friction for consumers, PSD2 is going in the opposite direction. Effective September 2019, PSD2 mandates strong customer authentication for the initiation of electronic payments, including e-commerce transactions. For card payments, PSD2 requires issuers to invoke multifactor authentication of their customers. The authentication must be based on at least two independent factors:

- **Knowledge:** Something only the customer knows, which may be a password or PIN. Recent guidance by the European Banking Authority (EBA) does not consider card data (e.g. card number or expiry date) as a knowledge factor.
- **Possession:** Something the customer has, for example a device or hardware token.
- **Inherence:** Something the customer is, for example a biometric such as fingerprint or facial recognition. The behavioral biometric is recognized by the EBA as a valid inherence factor.

The initial industry response to the SCA included a great deal of consternation about the impact it would have on e-commerce. Merchants and issuers were justifiably concerned that the friction would result in shopping cart attrition. As a result, the final RTS includes several exemptions, as follows:

- Transactions that are under 30 euros do not need to be challenged. While good for the customer experience, this transaction threshold will do nothing to stem the rampant card testing, in which organized crime rings test stolen cards with low-dollar-value transactions.
- The customer can whitelist trusted beneficiaries. SCA is required for the customer's first payment to the business but not for subsequent payments, with no limit to transaction amount.
- For card payments above 30 euros, payment service providers (PSPs) can use the exemption for transaction risk analysis. This allows PSPs to apply risk-based authentication and not apply SCA. The transaction risk analysis threshold depends on the PSP's fraud rates as follows:
    - If the fraud rate is below 13 basis points, there's no requirement for stepped-up authentication for transactions of up to 100 euros. If the fraud rate is below 6 basis points, the ceiling rises to 250 euros. For those with a rate of under 1 basis point, only transactions over 500 euros require stepped-up authentication. The fraud rate for the application of the exemption is calculated as the total value of unauthorized and fraudulent CNP transactions divided by the total value of all CNP transactions. This must be calculated for all card payments processed by the PSP within the European Economic Area.
    - Transaction risk analysis is applied by the acquirer and/or by the issuer. If the acquirer invokes the transaction risk analysis exemption, it will be liable for the payment in case of fraud.

    - Not all low-value transactions will go unchallenged; there are cumulative limits in place that require SCA when the limits are reached. Issuers have the choice to either challenge every fifth transaction (below 30 euros), or request SCA if the combined value of several unchallenged transactions goes above 100 euros. This could present some difficulty for merchants that will have to deal with customers' expectations of a frictionless process.
- If a recurring transaction is a regular payment that is the same amount every time, only one stepped-up authentication is required. If the amount changes (e.g., utility bills that are a different amount each month) and the amount is over 30 euros, it will need to be challenged.

As a result of this regulation, transactions that require authentication will significantly increase. Europe sees around 50% of its e-commerce transactions travel along the 3DS protocol, and the European issuers interviewed for this report expect to see this increase to the high 90s with the imminent PSD2 requirement for SCA.

KEY 3DS 2.0 CONSIDERATIONS FOR MERCHANTS

As the industry migrates to 3DS 2.0, merchants have four primary motivations. 3DS 2.0 has the potential to reduce false declines, increase authorizations, and shift the liability of fraud losses to the issuer. And in countries with a mandate for multifactor authentication for CNP transactions, 3DS provides a clear path to compliance. The ensuing sections discuss the key questions to consider as merchants enable 3DS 2.0.

WHAT WILL BE THE PERFORMANCE BENEFITS?

No surprise, a key question for most merchants as they evaluate 3DS 2.0 is what kind of performance benefit they can expect to reap. What will be the impact to false declines? By how much will authorizations increase? What decrease in fraud losses can be expected? How many transactions will see stepped-up authentication? Unfortunately, many of these questions don't yet have a definitive answer. Since the protocol is so new, no performance data exists yet. However, 1.0.2, with its risk-based authentication approach, can provide some informative leading indicators, as detailed below. These metrics should only improve as merchants send through the enriched data stream available with 2.0, which should result in better issuer decisioning.

- **Authorizations:** According to one of the payment networks, 3DS transactions using the old 3DS protocol generally see 10% to 11% higher authorization rates than non-3DS transactions in markets with widespread 3DS use. A large travel merchant in the U.S. (a market with limited 3DS use) that has deployed 3DS for the bulk of its volume says that it saw a 2.4% increase in authorizations compared to its pre-3DS authorization rates. The increase in authorization rates implies a commensurate decrease in false declines.

- **Fraud loss decrease:** The calculus on this front is easy—virtually all transactions that the merchant sends along the 3DS rails will benefit from the liability shift. There are some slight variations in what qualifies for 3DS among the different card brands and regions, so partnering with a vendor that can help navigate these nuances will be beneficial.

- **Stepped-up authentication rate:** Previous Aite Group studies have shown an average stepped-up authentication rate of 5% among issuers using the version 1.0.2's risk-based authentication capabilities.[7] This rate will likely decrease with the enhanced data stream from 3DS 2.0.

7. See Aite Group's report *Not Your Father's 3-D Secure: Addressing the Rising Tide of CNP Fraud*, February 2016.

WHEN IS THE RIGHT TIME?

The certification process for 3DS 2.0 is underway, so the right time for merchants to begin enabling the solution is now. Mastercard is requiring issuers in all markets to support 3DS 2.0 by October 2019. Issuers in nonregulated markets can comply with these standards by using the Mastercard Stand-In Risk-Based Authentication service. Issuers in regulated markets must be enrolled and compliant with the guidelines set forth in Mastercard's 3DS 2.0 program, known as Identity Check.

Irrespective of mandates, issuers are actively working to certify to the new protocol ahead of these deadlines. Issuers are also motivated by the potential to reduce false declines and improve the customer experience for their cardholders. As soon as both endpoints on a given transaction are 3DS 2.0-capable, the merchant's solution provider can invoke the new protocol. This again underscores the importance of selecting a vendor that has visibility into the broader 3DS ecosystem and an understanding of the nuances of 3DS 2.0 transactions.

WHAT ARE IMPORTANT 3DS 2.0 VENDOR ATTRIBUTES?

A key decision point for many merchants is how to enable 3DS 2.0. Here are some common criteria that merchants look for as they are enabling 3DS 2.0:

- **3DS expertise:** 3DS is a highly nuanced protocol. Merchants need help with a number of aspects, both at the time of implementations and on an ongoing basis, since the issuer side of the equation is rapidly evolving as well. Merchants need a vendor that can send their transaction over both the 3DS 1.0 and 2.0 rails (since both will be operating in parallel for at least a couple years). Merchants need a vendor that is able to view the stepped-up authentication method enabled by the issuer so it can decide how to proceed. Merchants also need a vendor that is well-versed in the 3DS nuances so it can understand whether the transaction is eligible for the liability shift (while the vast majority of transactions are, there are some regional and scheme-based nuances, especially around commercial cards).

- **Holistic risk assessment**: Merchants should look for vendors with a broad range of transaction risk capabilities. A range of frictionless risk assessment and authentication capabilities (such as device identity and behavioral biometrics) can help the merchant decide whether it wants to invoke 3DS in the first place, so it's important to look for a vendor that can support this.

- **Data optimization analytics:** From the merchant's perspective, the true potential of 3DS 2.0 lies in the ability of the enhanced data stream to reduce false decline rates. While some implementations allow merchants to restrict the amount of device information that is sent to the issuer, in many cases this will lead to higher friction on end users and lower approval rates. Merchants should look for vendors that can provide transparent dashboards and that can enable multivariate analysis of the benefit of sending incremental data.

- **Support for nonchallenge mode.** Another key enhancement in 3DS 2.0 is the ability for merchants to turn on 3DS in data-only mode. This offering gives merchants the

ability to share 3DS 2.0 data on non-3DS transactions to enable higher approval rates. Certain transactions do not make sense to invoke authentication. For example, if someone is playing a digital game, is getting attacked, and needs to buy new troops as soon as possible, this transaction may not make sense to send down normal authentication paths due to the response time and transaction value. Data-only mode enables merchants to share incremental data and not have to wait for an authentication response, but to instead immediately proceed to authorization with the benefit of the incremental data to boost the authorization rate. Mastercard further assists this process by providing the issuer with a score and reason code to further assist the issuer's authorization decision.

CONCLUSION

3DS is an important tool in the industry's arsenal against both CNP fraud and the false decline problem. Here are some recommendations for merchants as they are planning enablement of 3DS 2.0:

- **Look for solutions that can address the full transaction life cycle.** While leveraging the benefits of the new protocol is a key decision criterion, it's not the only one. Many merchants will only want to send a subset of their total transactions along the 3DS rails, so it's important to have a risk assessment solution that can perform frictionless detection and authentication prior to checkout to help determine which subset of transactions warrants the 3DS path.
- **Maximize the enhanced dataset.** More data means better decisions—merchants need to send as much data as possible along the new protocol to fully leverage the potential to reduce false declines, as well as to reduce the potential for stepped-up requests.
- **Educate your customer base.** Customers need to be trained to expect the occasional stepped-up authentication prompt so they know how to respond. Add messaging to your website to educate your consumer about what is happening when you send a transaction along the 3DS 2.0 rails.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

ABOUT NUDATA SECURITY

NuData Security is a Mastercard company that offers an easy-to-integrate package to access 3DS 2.0 combined with its award-winning seamless verification. NuData helps businesses identify users based on their online interactions and stops all forms of automated fraud before a critical decision. By analyzing over 350 billion events annually, NuData harnesses the power of behavioral and biometric analysis, enabling its clients to identify the human behind the device accurately across the entire session. This allows clients to block account takeover, stop automated attacks, and reduce customer insult. NuData's products are used by some of the biggest brands in the world to prevent fraud while offering a great customer experience.

CONTACT

For more information on NuData Security's products and services, please contact:

NuData Security Sales
verifygoodusers@nudatasecurity.com