Aite PARTNER. ADVISOR. CATALYST.

3-D Secure 2.0: Key Considerations for Card Issuers

FEBRUARY 2018

Prepared for:

RSA

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

It's no secret. As countries around the globe make the move to EMV, the organized crime rings behind financial fraud don't give up their criminal efforts and get a real job. They switch tactics, and card-not-present (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 fraud solutions designed to aid detection with a minimum of transactional friction, and 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 generally more troubling than potential fraud losses.[1]

3-D Secure 2.0 (3DS 2.0)[2] 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 Impact Note provides insight into the key factors that issuers need to take into consideration as they plan their move to 3DS 2.0.

METHODOLOGY

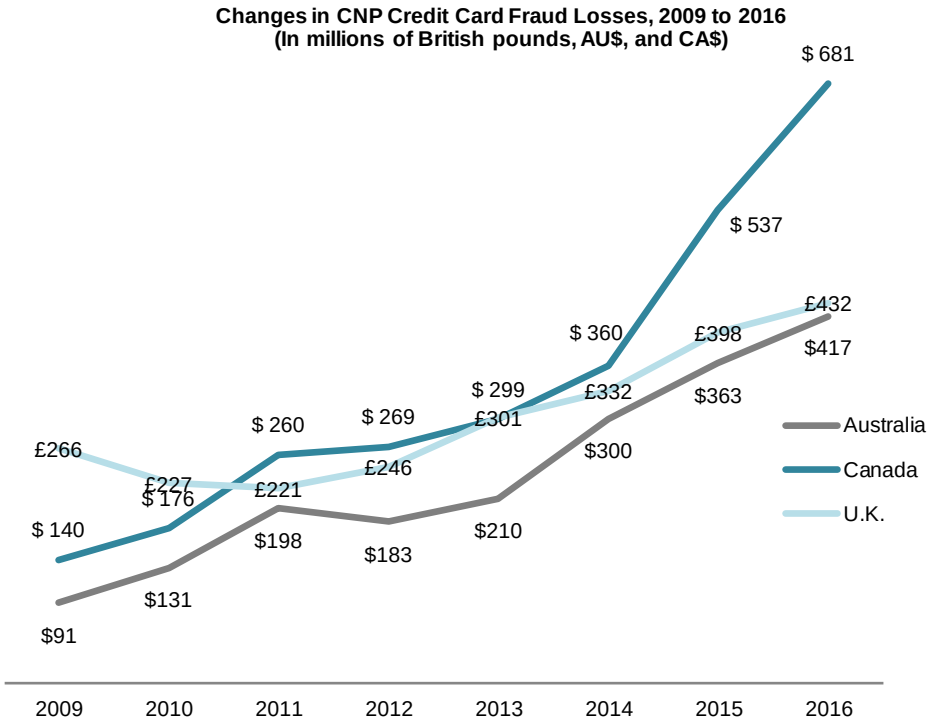
This white paper, sponsored by RSA Security, is informed by Q1 2018 interviews with global payment networks, issuers, merchants, and fraud mitigation vendors as well as ongoing conversations with executives in the space about their current and planned use of 3DS.

1. See Aite Group's report *Combating False Declines Through Customer Engagement*, May 2017.
2. 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 ever higher in countries around the globe (Figure 1).

Figure 1: Global CNP Fraud Losses



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

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

- **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.

3. See Aite Group's report *EMV: Issuance Trajectory and Impact on Account Takeover and CNP*, May 2016.

- **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

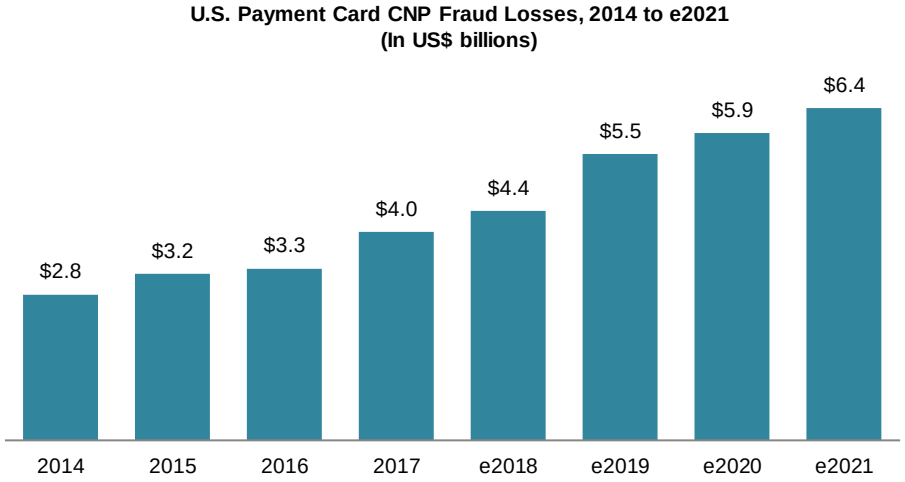
Country	E-commerce growth rate	Country	E-commerce growth rate
Australia	40%	**India**	17%
Turkey	31%	**U.K.**	16%
Mexico	26%	**Japan**	16%
Italy	26%	**Chile**	15%
Spain	25%	**South Korea**	15%
Russia	25%	**Brazil**	14%
Argentina	22%	**Saudi Arabia**	11%
France	21%	**Canada**	9%
Indonesia	20%	**U.S.**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

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 issuers and 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.[5] 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.
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.

5. See Aite Group's report *Combating False Declines Through Customer Engagement*, May 2017.

Market trends	Implications
Rapid growth of m-commerce	M-commerce is growing at a faster rate than the umbrella category of e-commerce. Global retail sales through the mobile phone grew a whopping 47% year-over-year from 2015 to 2016.[6]

Source: Aite Group

6. Paul Skeldon, "Boost in Mobile Commerce Sales Drives Ecommerce Growth in 2016 With More to Come This Year, Says IMRG," Internet Retailing, January 17, 2017, accessed on December 28, 2017, http://internetretailing.net/2017/01/boost-mobile-commerce-drives-ecommerce-growth-2016-come-year-says-imrg.

WHAT IS 3DS?

3DS is a protocol that was jointly developed by Visa and Arcot Systems in 1999 in an effort to add an additional layer of security to e-commerce transactions.[7] Mastercard, Discover, JCB International, and American Express all subsequently adopted the protocol as well. 3DS provides issuers with the ability to prompt consumers for authentication at the time of an e-commerce transaction.

3DS establishes a common communication protocol across the brands. Each of the networks 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 current version of 3DS (1.0.2) is much improved. One of the most important enhancements is 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 are fundamental gaps in the first version of the protocol that can only be addressed by releasing an entirely new version.

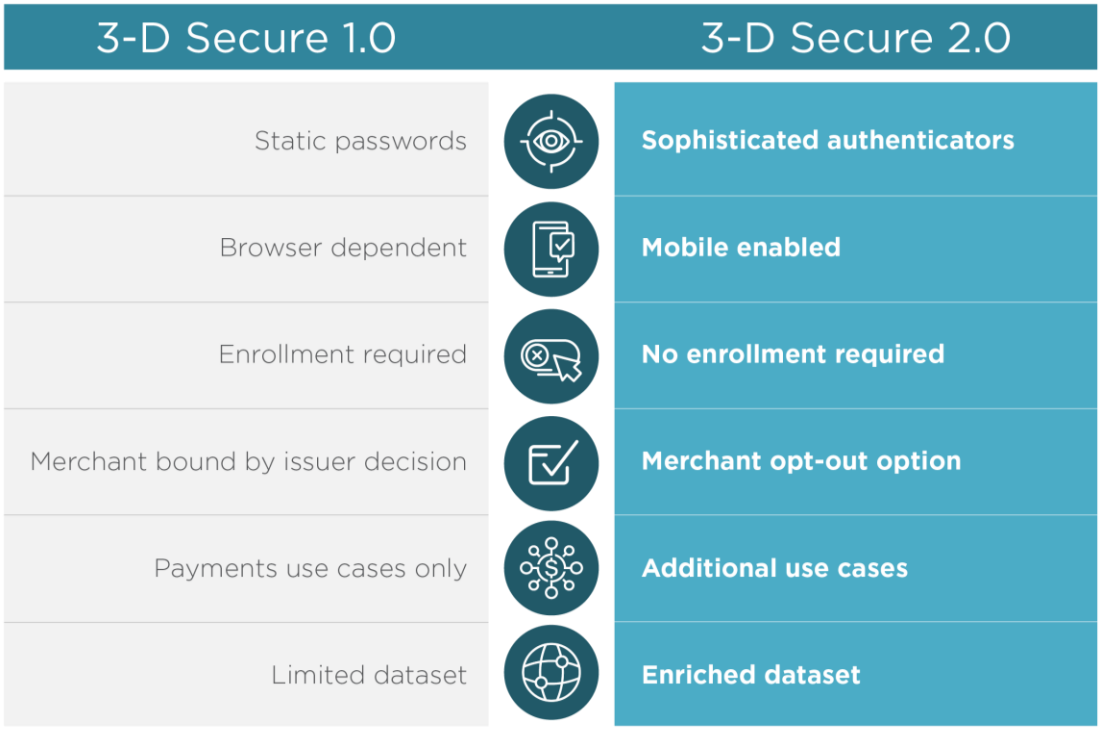
EVOLUTION TO 2.0

Visa ceded the 3DS intellectual property rights to EMVCo (which is jointly owned by American Express, Discover, JCB International, MasterCard, China UnionPay, and Visa) so that the protocol could be evolved at an industry level. After a lengthy collaborative process, EMVCo released the

7. For more background on 3-D Secure, see Aite Group's reports *Not Your Father's 3-D Secure: Addressing the Rising Tide of CNP Fraud*, February 2016, and *3-D Secure: Poised to Live Long and Prosper*, March 2013.

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, they're also not particularly user-friendly. 3DS 2.0 moves the protocol from static passwords to more 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 requirement that consumers actively enroll. Many of the vendors' risk-based authentication access control server (ACS) 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.[8]

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

8. For a comprehensive listing of the 3DS 2.0 data elements, see https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_210_1017.pdf

Data element	Required?	Definition
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
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 current 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 currently have 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 in order to reduce false declines while also better detecting fraud.

3DS 2.0 BENEFITS

The benefits of merchants adopting 3DS 2.0 include the following (the first three also exist with 3DS 1.0.2; the last is unique to 3DS 2.0):

- **Liability shift:** The fraud liability for transactions that travel across the 3DS protocol shifts from the merchant to the issuer.
- **Interchange reduction:** In many jurisdictions, the payment networks provide reduced interchange fees for 3DS-enabled transactions. Currently, all of the 3DS 2.0 economics are consistent with 3DS 1.0. At some point, 3DS 1.0 incentives will go away in order to incentivize merchants to migrate to 3DS 2.0, although no firm date has been established by the networks at this point.
- **Higher authorization rates:** 3DS transactions generally see 10% to 11% higher authorization rates than non-3DS transactions. Visa is providing the opportunity to further boost these rates by enabling visibility to authentication information in the authorization message. Mastercard has established a roadmap to provide a rich set of authentication insights in the authorization message on digital payment transactions.
- **Reduced false declines:** The enhanced data exchange promises to help issuers make better authorization decisions, putting a big dent in the false decline problem.

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

- **Better customer experience**: The combination of the enhanced data exchange and a risk-based authentication approach means fewer false declines as well as a reduction in stepped-up authentication requests for good customers. A card that is easier to transact with is more likely to stay top of wallet.
- **Reduced fraud**: The enhanced data and authentication will reduce CNP fraud. While issuers are not liable for CNP fraud losses if 3DS is not invoked, many are motivated to proactively tackle the problem to maintain high levels of service for their cardholders. This also translates to reduced costs as chargebacks decline,

and the contact center has fewer inbound calls related to CNP fraud and false declines.

- **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	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), 9402 (postal services—government only) If a merchant is not enrolled in VbV 3-D Secure 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.
	Mastercard	All transactions over US$200 require 3DS.
Brazil	Visa	Issuers must ensure that debit and Electron bank identification numbers (BINs) participate in VbV.

Country/ region	Mandating entities	Description
Canada	Visa and Mastercard	Issuers must ensure that business and consumer debit BINs participate in 3DS.
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. Effective April 2019, 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.[9] 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.
Japan	Japan Online Game Association	All association members are required to implement 3-D Secure.
New Zealand	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

9. "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 2016, accessed October 17, 2017, https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=10766.

Country/ region	Mandating entities	Description
		(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), 9399 (government services not elsewhere classified)
	Mastercard	All transactions over US$200 require 3DS.
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.
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.
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, the PSD2 requirement for SCA is going in the opposite direction. Effective September 2019, PSD2 mandates strong consumer authentication for the initiation of electronic payments, including (but not limited to) e-commerce transactions. The Regulatory Technical Standard (RTS) implementing this requirement has a series of criteria for what constitutes SCA.

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 included a number of 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. Financial institutions will have to watch for account takeover attacks that seek to exploit the whitelisting capability.

- For transactions above 30 euros, the requirement for authentication depends on the fraud rates of the acquiring bank and the issuer.
    - 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, that ceiling rises to 250 euros. For those with a rate of under 1 basis point, only transactions over 500 euros require stepped-up authentication.
    - Not all low-value transactions will go unchallenged: Every fifth transaction (below 30 euros) will need to be challenged. This will also apply 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 currently 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.

So what qualifies as SCA? This is another key question for many issuers, as it was a bit of a moving target during the SCA RTS finalization process. Passive technologies, such as device fingerprinting or behavioral biometrics alone, do not qualify. The SCA RTS requires that electronic payments are authenticated using two of the three classic multifactor categories of knowledge, possession, and inherence (i.e., something you know, something you have, and something you are). One issuer interviewed for this report said that there are rumors that SMS OTP was deemed noncompliant given criminals' ability to compromise it, but the interpretation of one of the payment networks interviewed is that it is acceptable under the current construct.

THE COMMERCIAL CARD CONUNDRUM

Commercial card issuers are faced with unique challenges when it comes to compliance with the SCA RTA. The regulation was constructed with consumer use cases in mind, and most of the recommended forms of authentication are not easily workable for commercial card use cases. Because of the high dollar value of the typical commercial card transaction, it would not qualify for the exemptions to the SCA requirement.

Commercial card is rife with use cases in which the one-to-one relationship between a cardholder and a transaction do not hold true. Corporate travel is a perfect example. In many cases, an administrative assistant or a central travel office is using a corporate card number to make a travel reservation on behalf of someone else. The issuer has no way of knowing who is conducting a transaction at that time and thus has no mechanism to perform the authentication.

While the European Banking Authority was strongly pushing for the SCA to apply to commercial cards in spite of the many challenges, the European Commission sided with common sense, and the final RTS exempts lodge cards, corporate cards, and virtual cards from the SCA.

ENABLING 3DS 2.0

To send transactions along the new protocol, all participants must go through the EMVCo testing and certification process. At this point, UL is the sole company authorized by EMVCo to conduct the certification, which has many of the interviewees wondering whether the industry will run into a certification bottleneck. Anticipating this, EMVCo is actively working to expand to additional vendors to support the testing and certification process.

The test facility will be ready to start certifying 3DS 2.0 early adopters in April 2018. First, the networks and their partners will certify their components. Once this is complete, they will begin onboarding early adopting customers, with a few weeks of testing required to certify each of these. The early adopter phase is expected to last around one quarter, then the protocol will be open to all participants. Visa's rules for 3DS 2.0 go into effect in April 2019 globally, while Mastercard has stated that all issuers must sunset the static password as the primary authentication method by December 31, 2018. The remainder of the Mastercard SecureCode program will sunset and be replaced by the new 3DS 2.0 Identity Check authentication program on December 31, 2019.

While these timelines seem straightforward, they have been a bit of a moving target since the 3DS 2.0 specification was first published in October 2016. One of the Australian issuers interviewed for this report says that its understanding is that issuer participation in its region is mandated for April 2018, and until it is advised otherwise, it will keep aiming toward that target. Since EMVCo is not opening up the certification process until April 2018, however, it is highly unlikely that the Australian April 2018 deadline will hold.

KEY 3DS 2.0 CONSIDERATIONS FOR ISSUERS

As the industry migrates to 3DS 2.0, issuers have two primary motivations. In regulated jurisdictions, 3DS provides a clear path to compliance. And in both regulated and nonregulated areas, 3DS 2.0 has the potential to provide cardholders with a better user experience, thus helping the issuer stay top of wallet. The ensuing sections discuss the key considerations as issuers are moving to 3DS 2.0.

IF WE BUILD IT, WILL THEY COME?

A consistent question in the issuer discussions was the willingness of merchants to participate and how much data they will send. A significant amount of the enriched data set is optional, so the ability of 3DS 2.0 to live up to its promise of increased authorizations will depend on the amount of data merchants transmit. The promise is there—approval rates for 3DS 1.0 transactions are already 10% to 11% higher in regulated markets in which 3DS is widely used. Those rates should increase substantially with 10 times more data feeding the decisioning systems. In markets where the use of risk-based authentication is already widespread, issuers and merchants also see faster checkout times, reduced fraud, and less friction compared to the original, static version of 3DS.

In countries where 3DS is not required, the extent to which merchants are willing to participate is an open question. Less than 2% of North American e-commerce transactions and fewer than 5% of Australian transactions use 3DS today. The Australian 3DS rate will increase substantially in April 2019 when Visa's requirements for VbV for a large swath of MCC codes goes into effect (Table E).

While the promise of higher authorization rates is a powerful incentive, merchants remain wary of the attrition that could result from friction in the transaction. One issuer suggests that the protocol should be renamed in order to remove the stigma associated with the challenges for 3DS 1.0. Merchants' views of 3DS vary widely depending on their business model and the type of goods sold. One shared economy merchant says that it will "never use 3DS," as any form of transactional friction would be disastrous for its business model. Conversely, a digital goods merchant that is struggling with high false decline rates is actively working on its 3DS 2.0 migration plan.

One of the issuers interviewed for this report plans to engage key merchants in its footprint in value tests to prove the value of sending incremental data. If the merchant sends a sample of data with enriched data, the issuer plans to run the transaction set through its models and will share the delta. It is also offering to pilot the system with key merchants and share the results to incentivize merchant participation.

MIGRATION PATH

Three types of issuers are moving to 3DS 2.0:

- Issuers that are on a non-risk-based version of 3DS 1.0

- Issuers that are not yet enabled for 3DS
- Issuers that are on a risk-based version of 3DS 1.0

For issuers that are currently enabled for RBA via a third-party vendor, the basic migration to 3DS 2.0 should not be overly onerous. The issuer's current ACS provider will do most of the heavy lifting in terms of integrating the new data elements. That said, one of the chief concerns among issuers interviewed for this report is that information about what the migration entails has not been readily available from all ACS providers.

If the issuer chooses to bring elements of the enriched data set into the authorization flow as part of its 3DS 2.0 migration, that entails a good deal of incremental effort and testing. Most large issuers use sophisticated card management systems that feed into decisioning systems, so any change to those will require extensive testing to ensure that the right fields are going through to the right systems. Not all issuers plan to do this out of the gate, however; all of the issuers interviewed for this report indicate that they will address the authorization message in a future phase, preferring to walk before they run.

Issuers that are on a non-risk-based version and those that are not yet enabled for 3DS are in the same position—both groups need to find a provider that can enable the risk-based flow of 3DS 2.0. Key considerations for these issuers as they evaluate providers are performance and cost.

COST

Cost is obviously a key component of any business case. Issuers in regulated jurisdictions don't have much choice in the matter. For issuers in nonregulated areas, the business case to justify the investment typically rests on the improvement to the customer experience and fraud prevention. Customer experience can be harder to quantify, although the revenue benefits associated with increased transaction volume and customer retention are two key metrics issuers use in business cases.

Fraud prevention is a bit more tangible, especially if the issuer does not have 3DS enabled today and is on the receiving end of transactions that merchants are sending along the protocol. If the transaction is sent along 3DS by the merchant, the issuer bears liability for it regardless of whether or not it has the ability to authenticate. Many merchants are already leveraging CardinalCommerce's rules engine that provides merchants with a BIN look-up table that enables them to determine to which issuers they want to send 3DS transactions. It flags issuers that do not have the ability to support 3DS; if an issuer cannot support 3DS, and the merchant sends the transaction along the 3DS rails, it will still benefit from the liability shift without the risk of any stepped-up authentication. This engine is causing many issuers that are on the receiving end of these transactions to prioritize implementation of 3DS.

PERFORMANCE

Performance is the primary driver of most issuers' choice of ACS. The three key metrics to consider here are fraud detection rates, false positive rates, and the intervention percentage (i.e., what percentage of transactions see a stepped-up authentication prompt). The existing ACS providers will have historical performance data that can show what level of fraud detection can

be expected at a given rate of intervention. For example, RSA's performance charts show a 97% fraud detection rate with 5% of transactions prompted for stepped-up authentication in 2017.

The big question is how these rates will improve as the industry migrates to 3DS 2.0. The enriched data set should significantly reduce the need for intervention while improving false positive rates. Proofs of concept with merchants will be required to determine exactly how much improvement will result.

STEPPED-UP AUTHENTICATION METHOD

The industry welcomes the move beyond static passwords, which are largely ineffective against fraud due to widespread data breaches and also entail a fair amount of customer friction. As issuers migrate to more complex authenticators, though, they need to choose wisely. The strength of the authenticator against fraud attacks, the ability for the authenticator to be used widely, the required amount of customer education, and the regulatory environment surrounding the authentication method are all important considerations.

Many of the issuers interviewed for this report are using SMS OTPs or plan to do so as part of their migration to 3DS 2.0. SMS has the advantage of ubiquity and customers having a good understanding of SMS OTPs. Unfortunately, criminals also have a good understanding of how to defeat SMS OTPs. A large Mexican issuer is the unfortunate poster child for this, absorbing over 200 basis points in 3-D Secure-related losses because criminals were having such an easy time defeating the SMS OTPs with SIM swaps.

Challenges can also arise if the issuer operates in multiple countries. SMS delivery can vary by mobile network operator (MNO). One issuer had a number of fire drills related to SMS nondelivery when it first started using SMS OTPs for 3DS authentication. In one case, a few countries' MNOs determined that they would only deliver messages when there was an actual number in the sender line, which resulted in nondelivery since this issuer had coded the messages so the customer would see the bank name in the sender line. This issuer has had issues with MNOs blocking delivery of text messages originating from out-of-country phone numbers. While all of these issues were addressed, they still occasionally resurface when the ACS's SMS provider makes a code change without appropriate change management controls, which causes old issues to resurface.

Mastercard is advocating biometrics as the stepped-up authenticator. In Europe, Mastercard issued a mandate requiring that all issuers support biometrics for online transactions by April 2019.[10] Whatever the authentication mechanism, it will be important for issuers to educate customers so that they are prepared for the stepped-up authentication prompts and know how to respond. Equally important will be educating customers about the types of social engineering scams that fraudsters will deploy in an effort to use this period of change to trick consumers into revealing their personal information.

10. "Mastercard Establishes Biometrics as the New Normal for Safer Online Shopping," Mastercard, January 22, 2018, accessed January 26, 2018, https://newsroom.mastercard.com/eu/press-releases/mastercard-establishes-biometrics-as-the-new-normal-for-safer-online-shopping.

CONCLUSION

3-D Secure is an important tool in the industry's arsenal against both CNP fraud and the false decline problem. Here are some recommendations for issuers as they are planning their migration to 3DS 2.0:

- **Engage with your ACS provider to determine what you need to do.** The major ACS providers will be part of the early adopter certification program, and they will be able to inform issuers about what is required for migration. If an issuer does not yet have an ACS, it should select one with a good track record with risk-based authentication that can provide a range of stepped-up authentication options and can clearly explain how its models help maximize detection and minimize false declines.
- **Prioritize feeding the data into your authorization system.** The enriched data flow will not only help improve authentication rates but will also help with authorization. It's understandable that issuers will want to walk before they run, but feeding data to the authorization routines should be on the roadmap for all issuers to maximize the effectiveness of 3DS 2.0.
- **For European issuers, develop a whitelist process to minimize friction.** While SCA will represent the potential for additional friction, an effectively managed and communicated whitelist process will minimize the impact.
- **Collaborate with key merchants to demonstrate the value of incremental data.** Follow the example of the large issuer interviewed for this report and engage with some large merchants to do a proof of concept that shows the impact that incremental data will have on the authentication and authorization rates. This will help cut through some of the uncertainty surrounding the new protocol.
- **Educate your customer base.** Customers need to be trained to expect the occasional stepped-up authentication prompt so they know how to respond. Effective customer training will not only reduce the potential for abandonment but will also help customers differentiate between the genuine 3DS authentication prompt and social engineering attacks by fraudsters.

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 RSA

RSA, a Dell Technologies business, offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world. For more information, go to rsa.com.

RSA 3-D SECURE 2.0 SOLUTIONS FOR ISSUERS

As an ACS provider for the 3DS 1.0.2 protocol, RSA Adaptive Authentication for eCommerce has already been delivering on many of the benefits of the 3D Secure 2.0 specification for nearly a decade. For example, RSA's risk-based approach eliminates cardholder enrollment, static passwords, and the 100% challenge rate to provide a largely frictionless experience. It supports biometrics, transaction signing, and out-of-band authentication with SMS and push OTP, among other authentication methods. It works across web and mobile channels, bringing together information about behaviors, devices, and known fraud to minimize losses from high-risk transactions.

The RSA Risk Engine is at the heart of the service and analyzes more than 100 fraud indicators to assess transaction risk. Its risk scores are also informed by the RSA eFraudNetwork, a repository of confirmed fraud data gleaned from RSA's research lab, ISPs, third party contributors across the globe, and RSA's network of customers.

Because of the accuracy of the RSA Risk Engine, users of the service are seeing excellent results. In 2017, Adaptive Authentication for eCommerce achieved the following:

- **Fraud detection:** A 97% detection rate at a 5% intervention rate (the average intervention rate across the existing customer base).
- **Average fraud rate:** 0.035% (3.5 basis points), or just $3.55 loss for every $10,000 in genuine orders approved.
- **Average intervention ratio (genuine:fraud):** Just 2.4 genuine transactions singled out for every fraud attempt blocked, compared with industry ratios that often fall with the range of 10 to 20 interventions for every fraud blocked.