Aite PARTNER. ADVISOR. CATALYST.

EMV 3-D Secure: Enhanced Data Driving Better Customer Experiences

DECEMBER 2018

Prepared for:

ca technologies A Broadcom Company

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
INTRODUCTION 4
  METHODOLOGY 4
RISING CNP FRAUD AND FALSE DECLINES 5
WHAT IS EMV 3DS? 8
  EMV 3DS BENEFITS 10
  3DS: A GLOBAL SNAPSHOT 14
  THE PATH FORWARD: BETTER SECURITY, FEWER FALSE DECLINES 14
CONCLUSION 16
ABOUT AITE GROUP 17
  AUTHOR INFORMATION 17
  CONTACT 17
ABOUT CA TECHNOLOGIES 18

LIST OF FIGURES

FIGURE 1: GLOBAL CNP FRAUD LOSSES 5
FIGURE 2: U.S. CNP FRAUD 6
FIGURE 3: CONSUMERS’ REACTIONS TO FALSE DECLINES BY COUNTRY 7
FIGURE 4: TARGET OF CONSUMER FRUSTRATION BY COUNTRY 7
FIGURE 5: DIFFERENCES BETWEEN 3DS 1.0 AND EMV 3DS 8
FIGURE 6: 3DS USE ACROSS THE GLOBE 14
FIGURE 7: CONSUMERS’ ATTITUDES TOWARD CONTROL OVER SECURITY 15

LIST OF TABLES

TABLE A: EMV 3DS DATA ELEMENT SAMPLES 9
TABLE B: MULTIFACTOR AUTHENTICATION MANDATES 11

EXECUTIVE SUMMARY

EMV 3-D Secure: Enhanced Data Driving Better Customer Experiences, commissioned by CA Technologies and produced by Aite Group, explains the benefits of adopting 3-D Secure 2.0 (EMV 3DS) for card issuers. Key takeaways from the study include the following:

- Compared with the legacy 3DS 1.0 solution, EMV 3DS provides significant improvements, which are expected to increase authorization rates, reduce card-not-present (CNP) fraud, and provide a better customer experience relative to 3DS 1.0.
- EMV 3DS provides an enhanced data stream between issuers and merchants to better inform decisioning. The data available for merchants to send issuers increases from the 15 data fields supported by 3DS 1.0 to more than 150 data fields in EMV 3DS. This promises to significantly reduce false declines as well as decrease fraud losses.
- The new protocol is mobile-friendly, an important attribute as mobile commerce continues to grow rapidly in countries around the globe.
- EMV 3DS provides a clear path to compliance in the increasing number of regions and countries that require multifactor authentication for CNP transactions.
- As issuers work toward EMV 3DS enablement, they should look for a vendor well versed in the nuances of 3DS. Enabling vendors should bring a good track record with risk-based authentication, a range of stepped-up authentication options, and should clearly be able to explain how their models can help maximize detection and minimize false declines.

INTRODUCTION

Banking and commerce activity is increasingly originating from digital endpoints—computers, smartphones, tablets, and even voice assistants such as Alexa. While this represents new and interesting opportunities for engagement, these digital channels also require a robust and evolving set of fraud detection, authentication, and authorization mechanisms.

The big challenge facing issuers is how to deploy the optimal mix of technology that can detect the bad activity and minimize false declines while also providing a positive customer experience. All of this also needs to be done while complying with a vast patchwork of local regulations, many of which are increasingly mandating higher levels of security for CNP transactions.

EMV 3DS has the potential to be a key tool in issuers' arsenal. This new-and-improved version of the 3DS protocol introduces a number of improvements relative to 3DS 1.0:

- EMV 3DS offers an enhanced data stream between issuers and merchants to better inform authentication and authorization decisions.
- EMV 3DS expands the protocol beyond the browser into the mobile app environment.
- EMV 3DS eliminates the static password, instead requiring more secure and user-friendly authenticators, such as one-time passwords (OTPs) and biometrics.

This white paper describes the significant differences between 3DS 1.0 and EMV 3DS, and provides insight into the key considerations for issuers as they plan their move to EMV 3DS.

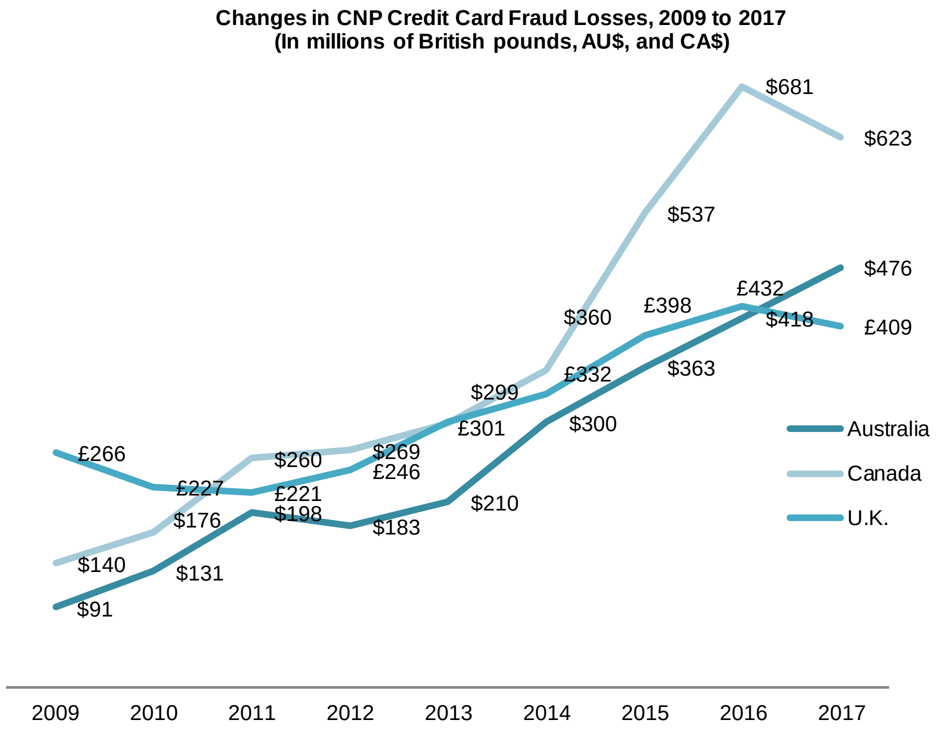
METHODOLOGY

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. It also leverages data from a July 2018 Aite Group survey of 1,400 consumers in the U.K., the U.S., and Singapore. The consumer survey sample is in proportion to each country's population for age, gender, income, geographic region, and race, and has a margin of error of three points at the 95% level of confidence.

RISING CNP FRAUD AND FALSE DECLINES

Rising e-commerce transaction volumes, combined with organized crime rings' effectiveness and efficiency at breaching and monetizing stolen data, is driving CNP fraud losses up around the globe (Figure 1). The global migration to chip cards has also resulted in a shift from fraud attacks that focus on the point of sale to attacks that increasingly focus on digital channels.

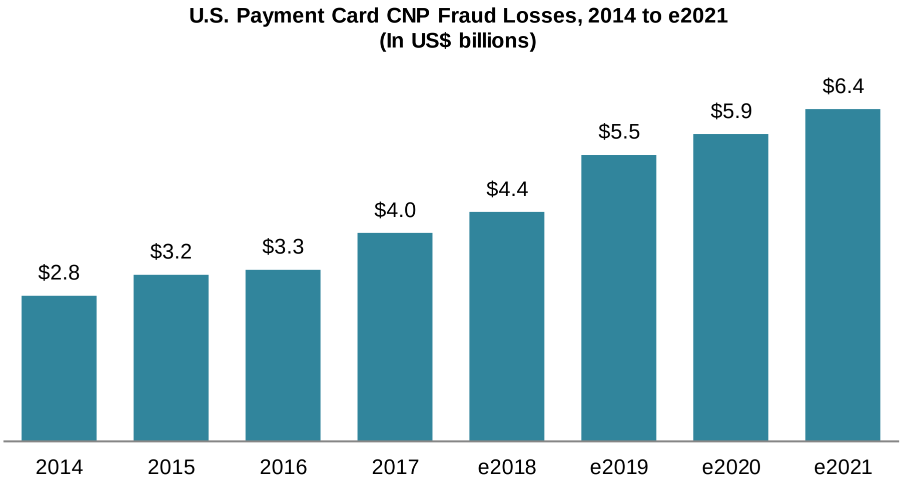
Figure 1: Global CNP Fraud Losses



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

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

Figure 2: U.S. CNP Fraud Losses



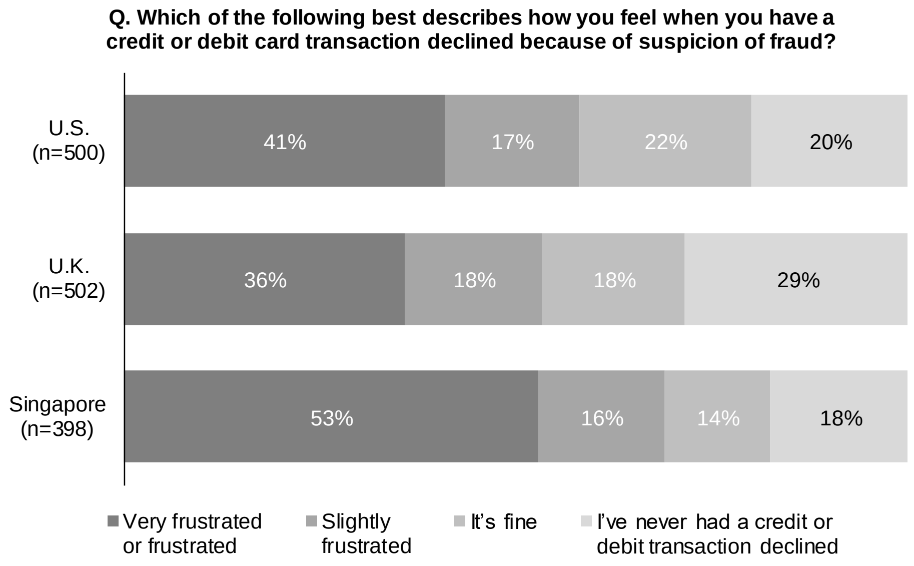
Source: Aite Group

For many issuers, however, false declines and the resulting “customer insults” are more troubling than the CNP fraud itself. 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, Aite Group estimates that false declines for payment card transactions will exceed US$330 billion in 2018. The CNP channels are disproportionately impacted by false declines, with the average decline rate for a CNP transaction hovering around 15% to 20%, compared with 2% to 3% for card-present transactions.

Consumers don’t like false declines either, for obvious reasons. More than half of consumers across the countries surveyed by Aite Group feel frustrated when a false decline occurs, with Singapore consumers showing the least tolerance for false declines, aka “customer insults” (Figure 3).

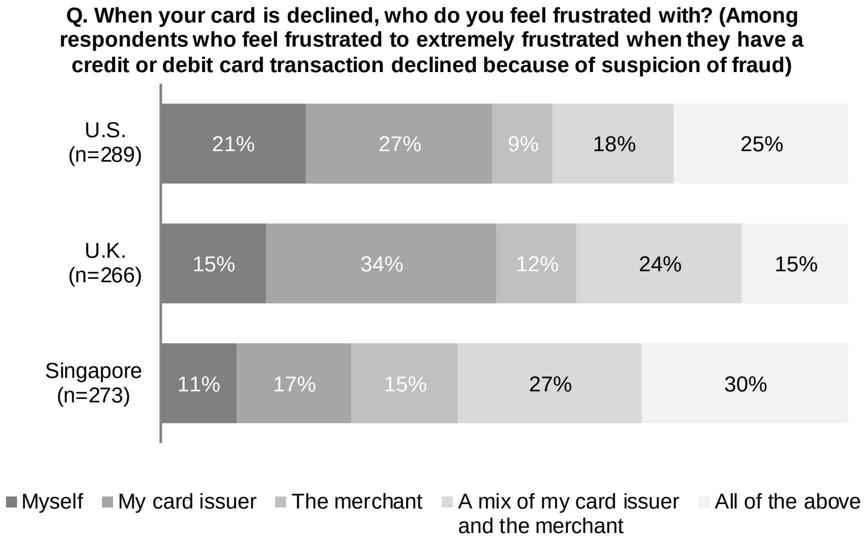
Figure 3: Consumers' Reactions to False Declines by Country



Source: Aite Group survey of 1,400 consumers in the U.K., the U.S., and Singapore, July 2018

The card issuer is the primary target of consumers' frustration, as shown in Figure 4.

Figure 4: Target of Consumer Frustration by Country



Source: Aite Group survey of 1,400 consumers in the U.K., the U.S., and Singapore, July 2018

EMV 3DS, with a vastly enriched set of data traveling from the merchant and the issuer, promises to put a big dent in false declines while at the same time increasing detection of fraudulent CNP transactions.

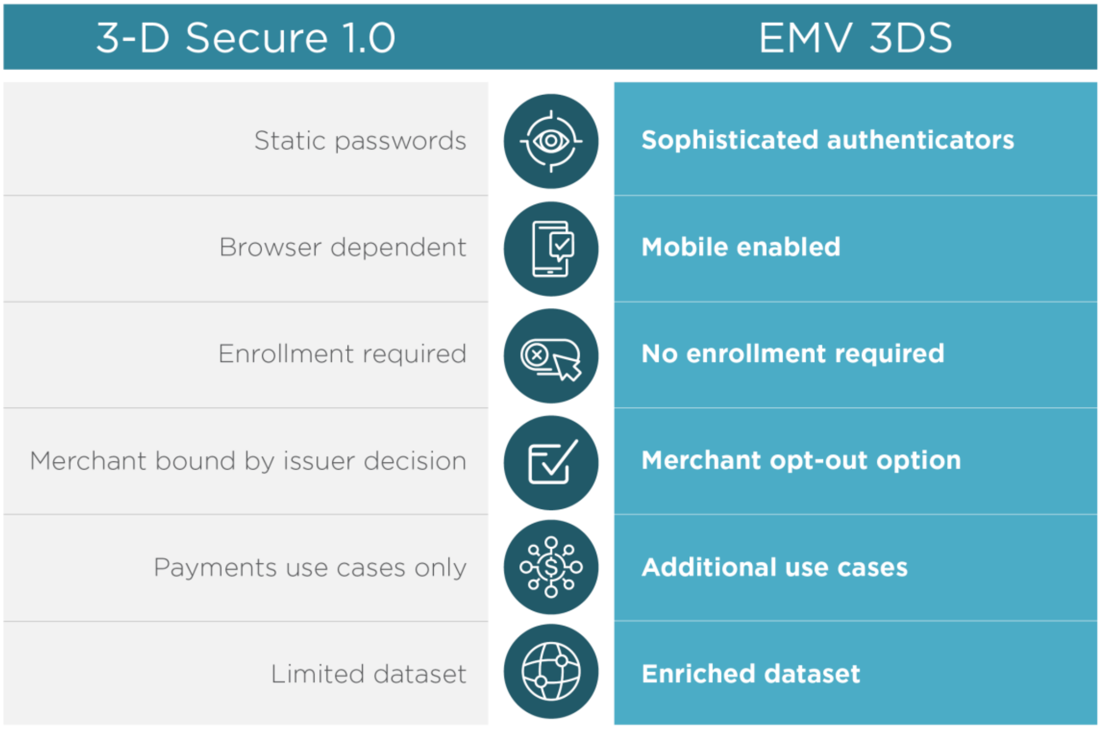
WHAT IS EMV 3DS?

EMV 3DS can help issuers address both false declines and rising CNP fraud. 3DS is a protocol managed by EMVCo that enables issuers to perform additional risk assessment at the time of a digital transaction and prompt the customer for additional authentication if the transaction appears risky. 3DS is a common communication protocol across card networks, which all have their separately branded programs and rule structures (e.g. Verified by Visa, Mastercard Identity Check). Issuers rely on access control server (ACS) technology provided by vendors such as CA Technologies for this advanced risk scoring; the benefit of EMV 3DS versus the initial version of 3DS is the vastly enhanced data that it supplies the engine.

Initially, 3DS 1.0 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. However, the payment networks and enabling vendors such as CA Technologies have made substantial changes to the process. One of the most important enhancements was the transition from a binary authentication approach, in which all transactions are subjected to a stepped-up authentication prompt, to 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.

After a lengthy collaborative process, EMVCo released the initial EMV 3DS specification in October 2016. The key differences between 3DS 1.0 and EMV 3DS are summarized in Figure 5 and are further elaborated below.

Figure 5: Differences Between 3DS 1.0 and EMV 3DS



3-D Secure 1.0	EMV 3DS
Static passwords	**Sophisticated authenticators**
Browser dependent	**Mobile enabled**
Enrollment required	**No enrollment required**
Merchant bound by issuer decision	**Merchant opt-out option**
Payments use cases only	**Additional use cases**
Limited dataset	**Enriched dataset**

Source: Aite Group

- **Sophisticated authenticators:** Not only are static passwords ineffective, but they're also not particularly user-friendly. EMV 3DS moves the protocol from static passwords to more robust authenticators, such as biometrics and OTPs.
- **Mobile enabled:** The smartphone and tablet had not been invented when the first version of 3DS was released, so the original protocol was entirely browser-based. EMV 3DS is capable of seamlessly integrating with both mobile app and browser-based environments, and the enhanced data stream helps reduce the number of times friction has to be inserted in a transaction.
- **No enrollment required:** EMV 3DS eliminates the active enrollment requirement. Many of the vendors' risk-based authentication 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 EMV 3DS 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). EMV 3DS provides this ability.
- **Additional use cases:** While 3DS 1.0 was built around the payment transaction, EMV 3DS supports additional use cases, such as account verification and token provisioning.
- **Enriched dataset:** 3DS 1.0 supports 15 data elements. The EMV 3DS dataset has significantly expanded with more than 150 data elements, of which some are required and others are optional or conditional. A sample of some of the incremental fields in the EMV 3DS data set is provided in Table A.[1]

Table A: EMV 3DS Data Element Samples

Data element	Required?	Definition
3DS requestor authentication method	Optional	Mechanism used by the cardholder to authenticate to the 3DS requester
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

[1] For a comprehensive listing of the EMV 3DS 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 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 a 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 the 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.

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. EMV 3DS finally provides a mechanism for merchants to share this data with issuers to reduce false declines while also better detecting fraud.

EMV 3DS BENEFITS

The benefits to issuers adopting EMV 3DS include the following:

- **Better customer experience:** The combination of the enhanced data exchange and a risk-based authentication approach means fewer false declines and 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 mandated or are in the process of mandating multifactor authentication for CNP transactions. EMV 3DS provides compliance with the majority of these mandates, as described in Table B.

Table B: Global Multifactor Authentication Mandates

Country/ region	Mandating entity	Mandate description
Australia	Visa	Until April 12, 2019: All credit, debit, and reloadable prepaid cards must be enrolled in Verified by Visa (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 that their merchants use VbV if they exceed the merchant fraud thresholds in any quarter. Effective April 13, 2019: Merchants must process an e-commerce transaction using VbV EMV 3DS if the transaction 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).

Country/ region	Mandating entity	Mandate description
		If a merchant is not enrolled in VbV EMV 3DS 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.
Bangladesh	Mastercard	All acquirers and merchants must support EMV 3DS 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.
China	Visa	Issuers' VbV programs must use dynamic authentication.
European Union	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 to 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 effective dates), Mastercard will require EU issuers, acquirers, and merchants to support EMV 3DS 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 over 2,000 rupees.[2] The 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 EMV 3DS by October 2019.
Japan	Japan Online Game Association	All association members are required to implement 3DS.

[2] "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, 2018, https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=10766.

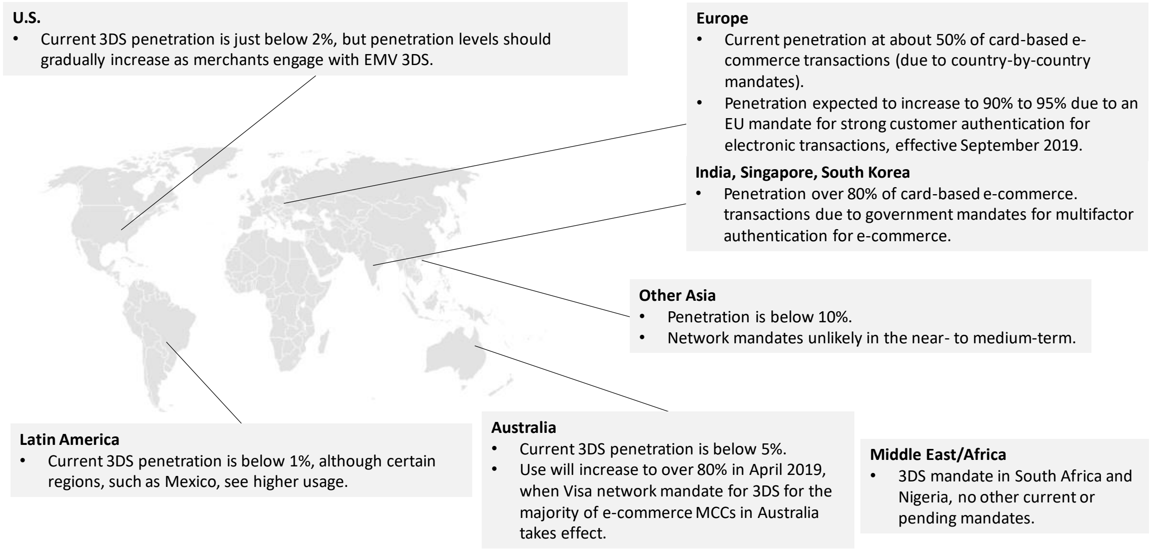
Country/ region	Mandating entity	Mandate description
Malaysia	Mastercard	All acquirers and merchants must support EMV 3DS by October 2019.
New Zealand	Visa	All Visa credit, debit, and reloadable prepaid cards must be enrolled in VbV. Virtual accounts associated with Visa commercial cards are excluded 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 (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).
	Mastercard	All transactions over US$200 require 3DS.
Nigeria	Visa	Nigerian issuers must ensure that 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 EMV 3DS by October 2019.
Singapore	Monetary Authority of Singapore	All online transactions must be authenticated with a dynamic OTP via 3DS.
South Africa	Payments Association of South Africa	All issuers and e-commerce merchants must support 3DS.
	Mastercard	All acquirers and merchants must support EMV 3DS 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

3DS: A GLOBAL SNAPSHOT

3DS penetration across the globe varies based on whether there are local requirements for multifactor authentication and market structure (i.e., whether the banking market is highly consolidated, making it easier for a handful of large banks that control the market to mandate strong authentication). Figure 6 provides a snapshot of current 3DS penetration levels around the globe.

Figure 6: 3DS Use Across the Globe



U.S.

- Current 3DS penetration is just below 2%, but penetration levels should gradually increase as merchants engage with EMV 3DS.

Europe

- Current penetration at about 50% of card-based e-commerce transactions (due to country-by-country mandates).
- Penetration expected to increase to 90% to 95% due to an EU mandate for strong customer authentication for electronic transactions, effective September 2019.

India, Singapore, South Korea

- Penetration over 80% of card-based e-commerce. transactions due to government mandates for multifactor authentication for e-commerce.

Other Asia

- Penetration is below 10%.
- Network mandates unlikely in the near- to medium-term.

Latin America

- Current 3DS penetration is below 1%, although certain regions, such as Mexico, see higher usage.

Australia

- Current 3DS penetration is below 5%.
- Use will increase to over 80% in April 2019, when Visa network mandate for 3DS for the majority of e-commerce MCCs in Australia takes effect.

Middle East/Africa

- 3DS mandate in South Africa and Nigeria, no other current or pending mandates.

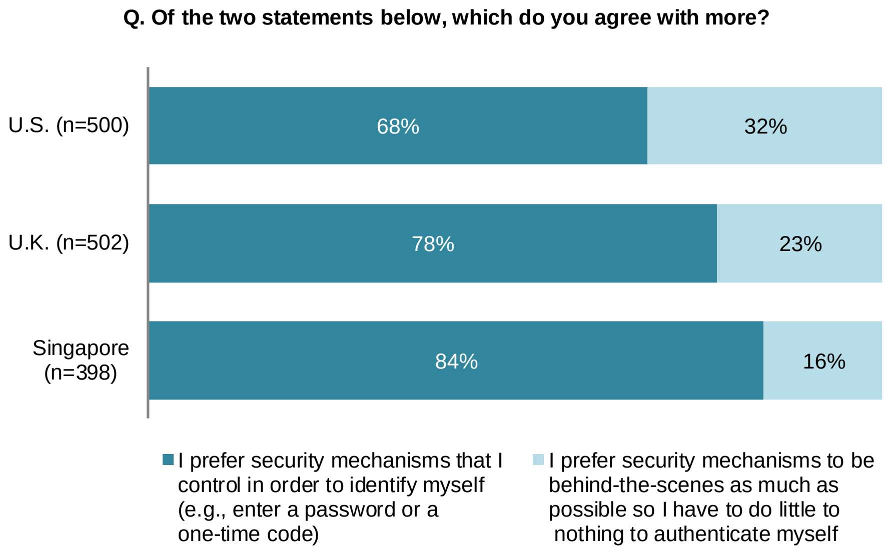
Source: Aite Group

THE PATH FORWARD: BETTER SECURITY, FEWER FALSE DECLINES

As the industry migrates to EMV 3DS, it can help improve CNP transaction performance on several fronts. EMV 3DS has the potential to reduce false declines, increase authorizations, and reduce fraud. And in countries with a mandate for multifactor authentication for CNP transactions, EMV 3DS provides a clear path to compliance.

Gone are the days when fraud was a topic that could be swept under the rug; customers are now well aware of it, and a secure commerce experience is table stakes. The majority of consumers also want to feel like they have an element of control over their digital commerce security, as shown in Figure 7.

Figure 7: Consumers' Attitudes Toward Control Over Security



Source: Aite Group survey of 1,400 consumers in the U.K., the U.S., and Singapore, July 2018

A key question for most issuers is what kind of performance benefits they can expect to reap. Unfortunately, since the protocol is so new, no EMV 3DS performance data exists yet. However, 3DS 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 3DS 2.0, which should result in better issuer decisioning.

- **Authorizations:** According to one of the payment networks, 3DS transactions 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 transaction volume said that it saw a 2.4% increase in authorizations compared with its pre-3DS authorization rates. The increase in authorization rates implies a commensurate decrease in false declines.

- **Fraud loss decrease:** By applying risk-based analytics, CA Technologies recently enabled a large global bank to reduce its false positives by 35% while increasing fraud detection by 25%.

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

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

CONCLUSION

EMV 3DS promises to help issuers reduce false declines and fraud and to comply with regional multifactor authentication mandates, while also providing a vastly improved customer experience compared with 3DS 1.0. Here are some recommendations for issuers as they plan enablement of EMV 3DS:

- **Look for a vendor well-versed in the nuances of 3DS.** Issuers should look for a vendor that has a good track record with risk-based authentication, that can provide a range of stepped-up authentication options, and that can clearly explain how its models can help maximize detection and minimize false declines. The vendor should also provide a sophisticated risk engine to effectively analyze the incremental data elements.

- **Prioritize feeding the data into your authorization system.** The enriched data flow will not only help improve authentication rates, but it 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 in order to maximize the effectiveness of EMV 3DS.

- **Educate your customer base.** Issuers need to set appropriate expectations about the potential changes to the customer experience so that when a stepped-up prompt does occur, the customer understands that the financial institution is trying to protect its customers, not inconvenience them.

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 CA TECHNOLOGIES

CA Technologies, a Broadcom company, is an industry leader in payment and identity fraud prevention, with friction-free transaction authentication powered by patented artificial intelligence. As a pioneer in data analytics for online fraud, CA Technologies delivers a unique 360-degree view of transactions for issuers, processors, and merchants across all payment schemes. Learn more at ca.com/issuers.