

EMV 3-D Secure: More Approvals, Fewer Losses for Merchants

NOVEMBER 2018

Prepared for:



TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
INTRODUCTION	4
METHODOLOGY	4
RISING CNP FRAUD AND FALSE DECLINES	5
WHAT IS EMV 3DS?.....	7
EMV 3DS BENEFITS	9
PSD2 SCA REQUIREMENT	13
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: DIFFERENCES BETWEEN 3DS 1.0 AND EMV 3DS.....	7
FIGURE 4: CONSUMERS' ATTITUDES TOWARD CONTROL OVER SECURITY	14

LIST OF TABLES

TABLE A: EMV 3DS DATA ELEMENT SAMPLES	8
TABLE B: MULTIFACTOR AUTHENTICATION MANDATES	10

EXECUTIVE SUMMARY

EMV 3-D Secure: More Approvals, Fewer Losses for Merchants, commissioned by CA Technologies and produced by Aite Group, explains the benefits of adopting EMV 3-D Secure (EMV 3DS). Key takeaways from the study include the following:

- EMV 3DS provides significant improvements to the legacy 3DS 1.0 solution, 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 fields supported by 3DS 1.0 to over 150 fields in EMV 3DS. This promises to better inform authorization decisions and reduce false declines.
- The new protocol is mobile-friendly, an important attribute as mobile commerce continues to grow rapidly around the globe.
- Another key enhancement in EMV 3DS is the ability for merchants to turn on 3DS in nonchallenge mode so that they can provide a frictionless customer experience while concurrently feeding the results into their own risk models and use that to inform their own approve/decline decisions.
- Some card schemes have advised merchants and issuers that EMV 3DS provides a clear path to compliance in the increasing number of regions and countries that require multifactor authentication for CNP transactions.
- As merchants work toward EMV 3DS enablement, they should look for a vendor well versed in the nuances of 3DS, which can provide a sophisticated data model and risk scoring to effectively analyze the incremental data elements. The enabling vendor should be able to inform the merchant about what type of stepped-up authentication (if any) the merchant should expect from the issuer on the other side of the transaction.

INTRODUCTION

Consumers' banking and commerce activity increasingly originates 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 merchants is how to deploy the optimal mix of technology that can both detect the bad activity and minimize false declines without disrupting the customer checkout flow and thereby damaging conversion rates and satisfaction. Piece of cake, right? 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 3-D Secure has the potential to be a key tool in merchants' 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 (OTP) and biometrics.

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

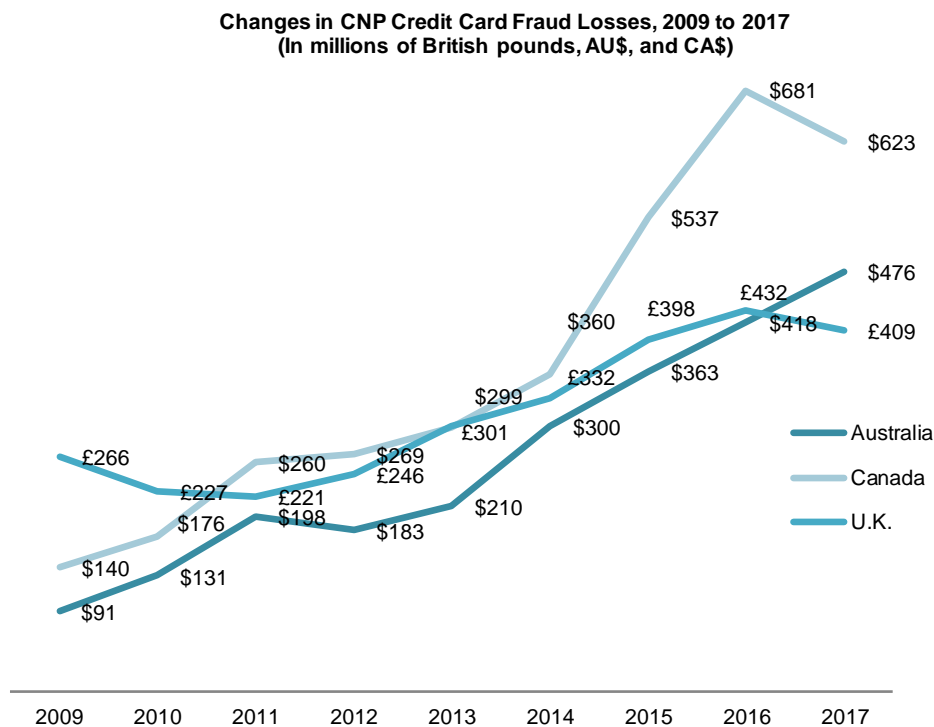
METHODOLOGY

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

The combination of rising e-commerce transaction volume and organized crime rings' effectiveness and efficiency at breaching and monetizing stolen data is driving CNP fraud losses up around the globe. The sophistication of attacks and ready availability of consumer data is also making certain types of fraud harder to detect. The global migration to chip cards has also resulted in a shift from fraud attacks focusing on the point of sale to attacks that increasingly focus on digital channels. While the data in Figure 1 seems to point to a potential reversal of this trend, the U.K. numbers aren't quite as rosy as they appear at first glance. The driver of the dip in overall U.K. CNP fraud losses was a 13% decrease in mail and telephone order (MOTO) fraud, while e-commerce fraud increased by 8% from 2016 to 2017.¹

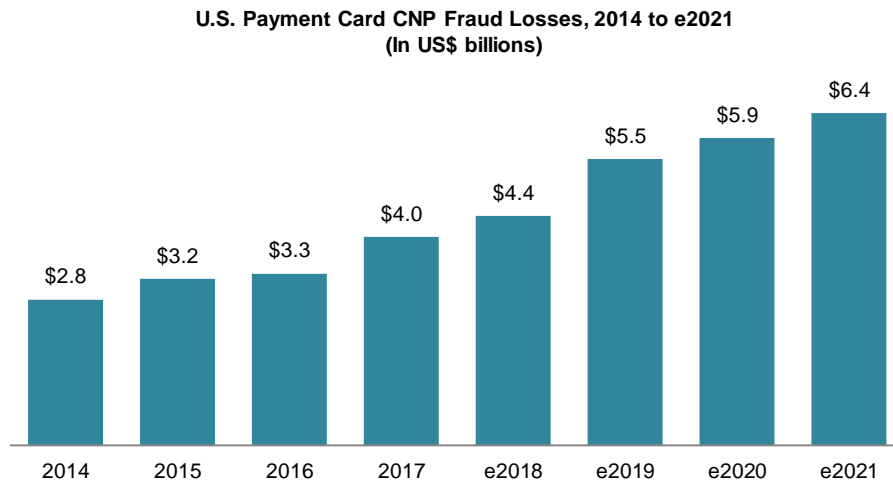
Figure 1: Global CNP Fraud Losses



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

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

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

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.







Aite Group estimates that false declines for payment card transactions will exceed US\$330 billion in 2018 in the U.S. market alone. The CNP channels are disproportionately affected 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.

WHAT IS EMV 3DS?

Using EMV 3DS can help merchants address false declines as well as rising CNP fraud. EMV 3DS is a protocol managed by EMVCo that enables issuers to perform additional risk assessment at the time of a digital commerce transaction and prompt the consumer for additional authentication if the transaction appears risky. 3DS is a common communication protocol across the card networks, which all have their separately branded programs and rule structures (e.g., Verified by Visa, Mastercard Identity Check).²

In its initial incarnation, 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. Over time, the payment networks and enabling vendors such as CA Technologies made substantial changes to the process. One of the most important enhancements was a transition from the requirement that all transactions are subjected to a stepped-up authentication prompt to the option of risk-based authentication, in which only transactions that fall into a specific risk threshold receive the stepped-up prompt. 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 3 and further elaborated below.

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

3-D Secure 1.0		3-D Secure 2.0
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

- The name 3-D Secure refers to the three domains that are involved in adding the additional layer of data transfer and security, which includes the acquirer or merchant domain, the issuer domain, and the interoperability domain, which facilitates the communication.

- **Sophisticated authenticators:** Not only are static passwords ineffective and often compromised, but they're also not particularly user-friendly. This can lead to high rates of transaction abandonment and loss of revenue. EMV 3DS moves the protocol from static passwords to more robust authenticators, such as biometrics and OTPs.
- **Mobile enabled:** The smartphone had not yet 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 mobile apps as well as browser-based environments.
- **No enrollment required:** EMV 3DS eliminates the requirement for consumers to actively enroll. Many of the vendors' risk-based authentication access control server solutions had already introduced this enhancement, so it was 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). EMV 3DS provides this ability.
- **Additional use cases:** While 3DS 1.0 was designed around the payment transaction, EMV 3DS supports additional use cases, such as account updates, verification, and token provisioning.
- **Enriched dataset:** The 3DS 1.0 protocol supports the transfer of 15 data elements. The EMV 3DS dataset has significantly expanded with more than 150 data elements, some of which are required while others are optional or conditional. A sample of some of the incremental fields in the EMV 3DS data set are found in Table A.³

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 requestor; for example, "no 3DS requestor authentication occurred" (i.e., cardholder "logged in" as guest) or "log in to the cardholder account at the 3DS requestor system using 3DS requestor's own credentials."
Browser IP address	Conditional	IP address of the customer's browser
Browser language	Required	Language used by the customer's browser

3. 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.

Cardholder account age indicator	Optional	Length of time that the cardholder has had the account with the 3DS requestor
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 total purchase amount 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

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 the mechanism for merchants to share this data with issuers in order to reduce false declines while also better detecting fraud and ensuring friction is minimized in order to maintain a positive customer experience.

EMV 3DS BENEFITS

The potential benefits to merchants adopting EMV 3DS include the following:

- **Liability shift:** The fraud liability for transactions that travel across the 3DS protocol shifts from the merchant to the issuer (as is the case with 3DS 1.0).
- **Interchange reduction:** In many jurisdictions, the payment networks provide reduced interchange fees for 3DS-enabled transactions. Currently, all the EMV 3DS economics are consistent with 3DS 1.0. At some point, 3DS 1.0 incentives will go away to motivate merchants to migrate to EMV 3DS.
- **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.
- **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: Multifactor Authentication Mandates

Country/ region	Mandating entities	Description
Australia	Visa	<p>Until April 12, 2019:</p> <p>All credit, debit, and reloadable prepaid cards must be enrolled in Verified by Visa (VbV).</p> <p>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.</p> <p>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.</p> <p>Effective April 13, 2019:</p> <p>Merchants must process an e-commerce transaction using VbV EMV 3DS 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).</p>

		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 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 effective dates), Mastercard will require European 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 above 2,000 rupees. ⁴ 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 EMV 3DS by October 2019.
Japan	Japan Online Game Association	All association members are required to implement 3-D Secure.
Malaysia	Mastercard	All acquirers and merchants must support EMV 3DS by October 2019.

4. "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>.

New Zealand	Visa	<p>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.</p> <p>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.</p> <p>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 and 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).</p>
	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.
	Mastercard	All acquirers and merchants must support EMV 3DS by October 2019.
Singapore	Monetary Authority of Singapore	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 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

PSD2 SCA REQUIREMENT

While EMV 3DS is moving in the direction of minimizing friction for customers, PSD2 is going in the opposite direction. Effective September 2019, PSD2 mandates SCA for electronic payments, including e-commerce transactions. All merchants doing business with European customers (not just those headquartered there) need to comply with this mandate. Some card schemes have advised merchants and issuers that EMV 3DS provides a clear path to compliance in the increasing number of regions and countries that require multifactor authentication for CNP transactions.

The initial industry response to the SCA mandate included a great deal of consternation about its impact on e-commerce. Merchants and issuers were justifiably concerned that the friction would result in a poor customer experience and shopping cart abandonment. As a result, the final requirement included 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 merchants. SCA is required for the customer's first payment to the business but not for subsequent payments, with no limit to transaction amount.
- 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, 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.
 - 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.

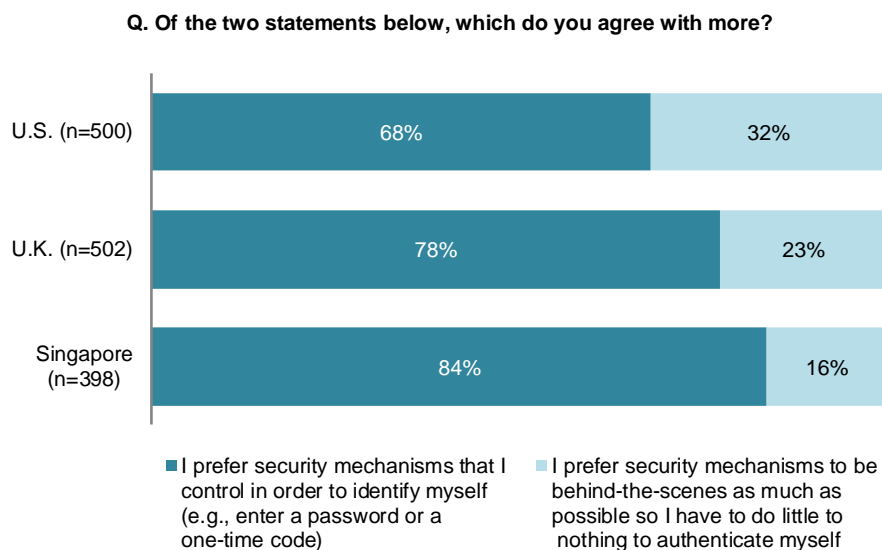
As a result of this regulation, transactions that require authentication will significantly increase. Europe currently sees around 50% of its e-commerce transactions travel along the 3DS protocol, but many issuers and payment network executives expect to see this increase to over 90% with the PSD2 requirement for SCA.

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 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.

Gone are the days when consumers were blissfully unaware of data breaches and fraud risk; consumers 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 4.

Figure 4: 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 merchants as they evaluate EMV 3DS 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, 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 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 region with limited 3DS use) that has deployed 3DS for the bulk of its 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:** 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 the 3DS liability shift among the different card brands and regions, so partnering with a vendor that can help navigate these nuances will be helpful.
- **Stepped-up authentication rate:** Previous Aite Group global studies have shown an average stepped-up authentication rate of 5% among issuers using the version 1.0.2's risk-based authentication capabilities.⁵ This rate will likely decrease with the enhanced data stream from EMV 3DS.

5. 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 merchants reduce false declines and fraud, comply with regional multifactor authentication mandates, and provide a vastly improved customer experience compared with 3DS 1.0. Here are some recommendations for merchants as they plan to enable EMV 3DS:

- **Maximize the enhanced data set.** More data means better decisions—merchants need to send as much data along the new protocol as possible to fully leverage the opportunity 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 customer about what is happening when you send a transaction along the EMV 3DS rails, and how this process benefits them.
- **Look for a vendor 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. It should also provide a sophisticated risk engine to effectively analyze the incremental data elements.

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 delivers a unique 360-degree view of transactions for issuers, processors, and merchants, across all payment schemes. Learn more at ca.com/merchants.