

# EMV 3-D Secure: The PSD2 Toolkit for European Issuers

DECEMBER 2018

Prepared for:



## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	3
INTRODUCTION .....	4
METHODOLOGY .....	4
RISING CARD-NOT-PRESENT (CNP) FRAUD AND FALSE DECLINES .....	6
WHAT IS EMV 3DS?.....	9
EMV 3DS BENEFITS .....	13
PSD2 STRONG CUSTOMER AUTHENTICATION REQUIREMENT .....	15
THE PATH FORWARD: BETTER SECURITY, FEWER FALSE DECLINES .....	17
CONCLUSION .....	19
ABOUT AITE GROUP.....	20
AUTHOR INFORMATION .....	20
CONTACT.....	20
ABOUT CA TECHNOLOGIES .....	21
ABOUT TSYS .....	22

## LIST OF FIGURES

FIGURE 1: GLOBAL CNP FRAUD LOSSES.....	6
FIGURE 2: U.K. CONSUMERS' REACTIONS TO FALSE DECLINES .....	7
FIGURE 3: TARGET OF CONSUMER FRUSTRATION IN THE U.K. ....	7
FIGURE 4: IMPACT OF FALSE DECLINES ON CUSTOMER ATTRITION .....	8
FIGURE 5: DIFFERENCES BETWEEN 3DS 1.0 AND EMV 3DS.....	9
FIGURE 6: EMV 3DS EUROPEAN MILESTONE DATES .....	14
FIGURE 7: MARKET ASSESSMENT OF EMV 3DS .....	15
FIGURE 8: CONSUMERS' ATTITUDES TOWARD CONTROL OVER AUTHENTICATION MECHANISMS .....	17

## LIST OF TABLES

TABLE A: EMV 3DS DATA ELEMENT SAMPLES .....	11
TABLE B: MULTIFACTOR AUTHENTICATION MANDATES IN EUROPE .....	13

## EXECUTIVE SUMMARY

*EMV 3-D Secure: The PSD2 Toolkit for European Issuers*, commissioned by CA Technologies and TSYS and produced by Aite Group, explains the benefits of adopting EMV 3-D Secure (EMV 3DS) for card issuers in Europe. Key takeaways from the study include the following:

- The liability shift for EMV 3DS is imminent: From April 2019, the card schemes will provide chargeback protection to merchants that have implemented EMV 3DS. As large online merchants are signing up as early adopters of EMV 3DS, issuers need to enable EMV 3DS themselves to avoid chargeback losses.
- EMV 3DS provides a clear path to compliance with the revised Payment Services Directive's (PSD2's) secure customer authentication (SCA) requirements. EMV 3DS also provides the right tools to minimise the impact of the SCA on the customer experience.
- EMV 3DS provides significant improvements to the legacy 3DS 1.0 solution. Critically, EMV 3DS provides an enhanced data stream between issuers and merchants to better inform decisioning. The wider and deeper data available for merchants to send to issuers increases from the 15 fields supported by 3DS 1.0 to over 150 data fields in EMV 3DS. This allows issuers to better assess risk during the authentication process and to approve transactions with higher confidence. EMV 3DS therefore has the potential to not only decrease fraud losses but also significantly reduce false declines.
- The new protocol is ready for all devices, including smartphones, tablets, and PCs. It is important that EMV 3DS is mobile-friendly as mobile commerce continues to grow rapidly in countries around the globe.
- As issuers work toward EMV 3DS enablement, they should look for a partner well-versed in the nuances of 3DS. Issuers should look for a partner 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 can help maximise detection and minimise false declines.

## INTRODUCTION

Consumers' 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 authorisation mechanisms. The big challenge facing issuers is how to deploy the optimal mix of technology that can detect the bad activity, minimise false declines, and provide a positive customer experience.

The 3DS message protocol supports issuers with additional security to online purchases by providing authentication between the cardholder and the issuer. The new EMV 3DS specification, as published by EMVCo, means a major upgrade of this standard that supports the use of mobile applications and allows issuers to make better informed authentication decisions.<sup>1</sup> As Mastercard and Visa have announced a liability shift by April 2019 for merchants that use EMV 3DS, issuers have to prepare for the migration to the new standard.

In Europe, issuers face the additional challenge of complying with PSD2. The European Banking Authority (EBA) mandates the use of SCA for all card payments (and other types of electronic payments) by September 2019.<sup>2</sup> Issuers are looking for ways to limit the impact of SCA for their customers, particularly for digital commerce.

EMV 3DS has the potential to be a key tool in the issuers' arsenal to achieve this. The new and improved version of the 3DS protocol provides an enhanced data stream between issuers and merchants to better inform authentication and authorisation decisions. This white paper describes the significant differences between 3DS 1.0 and EMV 3DS, and provides insight into the key considerations for European 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 recent Aite Group research, including the following:

- **July 2018 Aite Group survey of over 500 consumers in the U.K.:** The consumer survey sample is in proportion to the country's population for age, gender, income, geographic region, and race, and has a margin of error of 3 points at the 95% level of confidence.
- **Aite Group and Mobey Forum online survey (published November 2017):** This survey was directed at the methods available to balance risk management and

---

1. "EMV 3-D Secure Specification," EMVCo, accessed 8 October 2018, <https://www.emvco.com/media-centre/emv-3ds-press-kit>.

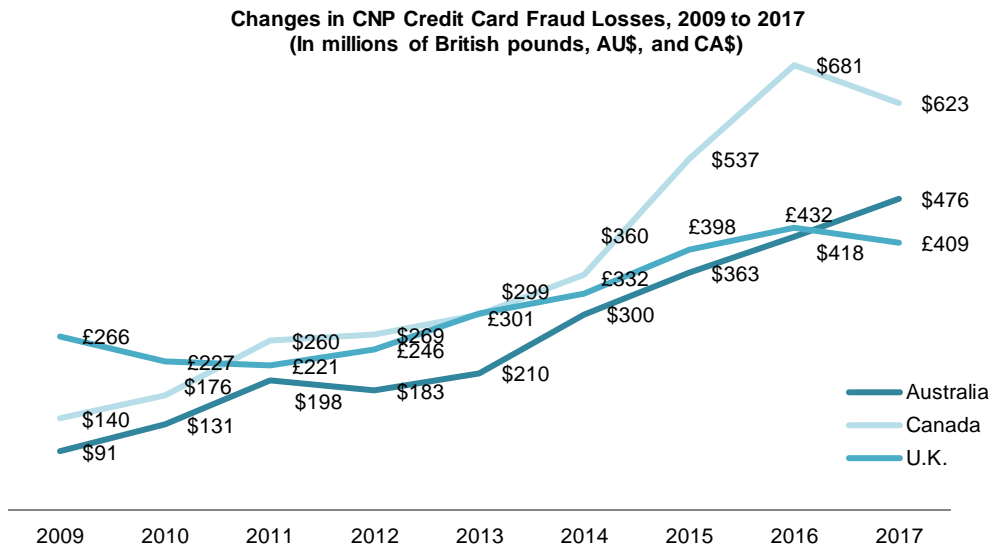
2. See Aite Group's report *PSD2 Regulatory Technical Standards: Content and Market Impact*, April 2017.

customer experience in mobile commerce. It has been produced by Aite Group in cooperation with Mobey Forum's expert group on strong customer authentication in m-commerce. The research is based on a survey held with 76 senior fraud and business-line executives at global financial institutions, payment networks, merchants, and fraud and authentication vendors.

## RISING CARD-NOT-PRESENT (CNP) FRAUD AND FALSE DECLINES

Rising e-commerce transaction volume combined with organised crime rings' effectiveness and efficiency at breaching and monetising stolen data is driving up CNP fraud losses around the globe (Figure 1).

**Figure 1: Global CNP Fraud Losses**



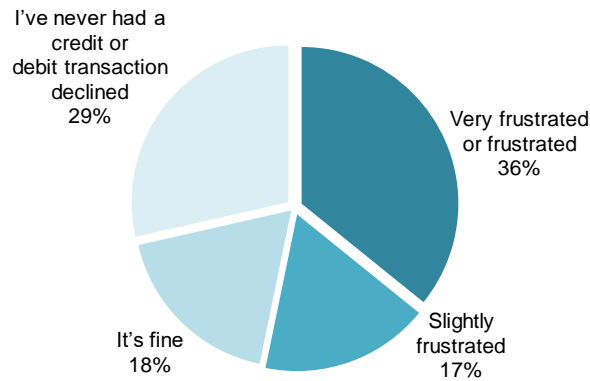
Source: Canadian Bankers Association, Financial Fraud Action U.K., Australian Payments Clearing Association

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. 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.

Consumers don’t like false declines either, for obvious reasons. From the group of consumers that had a transaction declined (71% of respondents), three out of four consumers felt frustrated with such an event (Figure 2).

## Figure 2: U.K. Consumers' Reactions to False Declines

Q. Which of the following best describes how you feel when you have a credit or debit card transaction declined because of suspicion of fraud? (N=502)

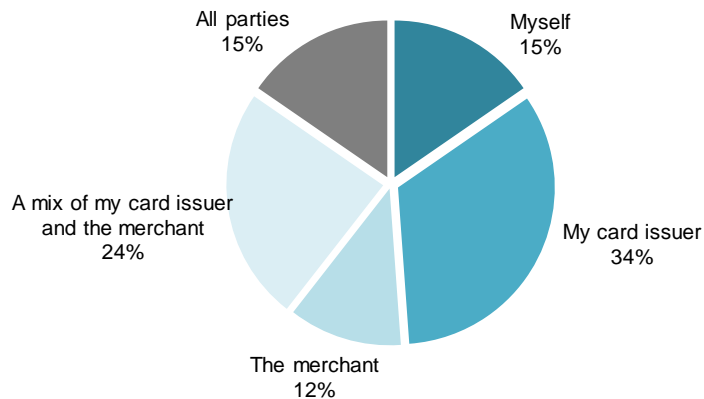


Source: Aite Group survey of 502 consumers in the U.K., July 2018

The card issuer is the primary target of consumers' frustration, as shown in Figure 3.

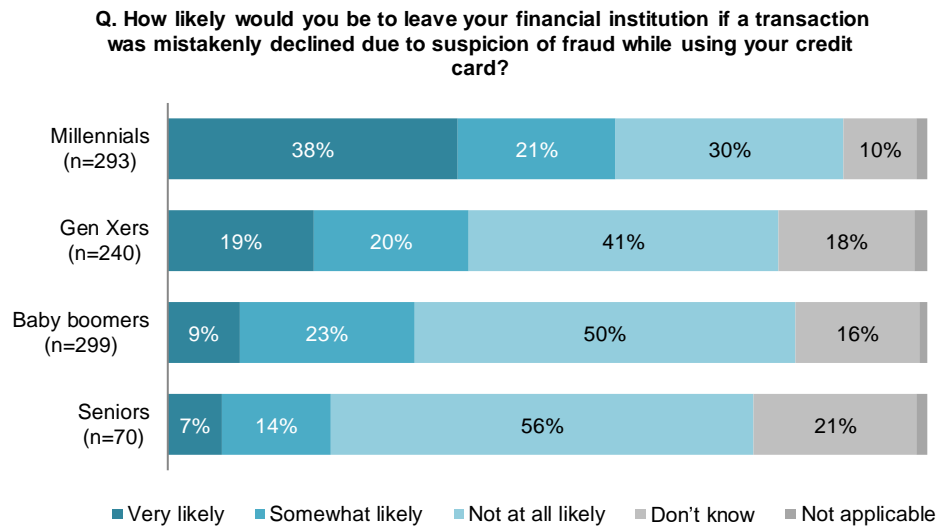
## Figure 3: Target of Consumer Frustration in the U.K.

Q. When your card is declined, whom do you feel frustrated with? (Among respondents who feel frustrated to extremely frustrated when they have a credit or debit card transaction declined because of suspicion of fraud) (N=502)



Source: Aite Group survey of 502 consumers in the U.K., July 2018

Therefore, issuers face a significant risk that customers will move their card to back of wallet in case of false positives. Evidence from the U.S. market indicates that this effect is strongest with millennials (Figure 4).

**Figure 4: Impact of False Declines on Customer Attrition**

Source: Aite Group survey of 1,095 U.S. consumers, January 2017

False declines by issuers or internal fraud management systems are a major issue for merchants that operate in highly competitive markets. Any false decline could lead to the loss of a customer for a long time. Aite Group research has shown that best-in-class merchants focus on the balance between a frictionless payment experience and fraud mitigation, and (closely controlled) fraud losses are acceptable if they reduce false declines and provide better bank authorisation rates.<sup>3</sup>

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

3. See Aite Group's report *The Strategic Importance of Merchant Payment Management*, February 2018.



## WHAT IS EMV 3DS?







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

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 partners made substantial changes to the process, and the last version of 3DS (version 1.0.2) was much improved.

One of the most important enhancements was to provide the option of risk-based authentication, removing the need to subject all transactions to stepped-up authentication. Even so, fundamental gaps in the first version of the protocol could only be addressed by releasing an entirely new version.

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

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

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

Source: Aite Group

- **Enriched dataset:** 3DS 1.0 supports 15 data elements. The EMV 3DS dataset 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 EMV 3DS dataset are found in Table A.<sup>4</sup>
- **Sophisticated authenticators:** 3DS 1.0 initially used static passwords to enroll customers into the service, leading to friction from cardholders forgetting their passwords. The protocol was later updated to support one-time passwords (OTPs). EMV 3DS supports the use of OTPs as well as more sophisticated authenticators such as biometrics. With the arrival of EMV 3DS, Visa and Mastercard will end the support of static passwords.
- **Mobile enabled:** The smartphone had not yet been invented when the first version of 3DS was released. EMV 3DS is capable of seamlessly integrating with mobile apps as well as browser-based environments.
- **No enrolment required:** EMV 3DS eliminates the requirement that consumers actively enrol. 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 formalised 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 them 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 verification and token provisioning.

---

4. For a comprehensive listing of the EMV 3DS data elements, see "Terms of Use," EMVCo, 4 April 2011, accessed 14 October 2018, [https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo\\_3DS\\_Spec\\_210\\_1017.pdf](https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_210_1017.pdf).

**Table A: EMV 3DS Data Element Samples**

<b>Data element</b>	<b>Required?</b>	<b>Definition</b>
<b>3DS requestor authentication method</b>	Optional	<p>Mechanism used by the cardholder to authenticate to the 3DS requestor</p> <p>Examples include the following:</p> <ul style="list-style-type: none"> <li>• 01 = No 3DS requestor authentication occurred (i.e., cardholder “logged in” as guest)</li> <li>• 02 = Log in to the cardholder account at the 3DS requestor system using 3DS requestor’s own credentials</li> <li>• 03 = Log in to the cardholder account at the 3DS requestor system using federated ID</li> <li>• 04 = Log in to the cardholder account at the 3DS requestor system using FIDO authenticator</li> <li>• 05 = Log in to the cardholder account at the 3DS requestor system using third-party authentication</li> <li>• 06 = Log in to the cardholder account at the 3DS requestor system using FIDO authenticator</li> </ul>
<b>Browser IP address</b>	Conditional	IP address of the customer’s browser
<b>Browser language</b>	Required	Language used by the customer’s browser
<b>Cardholder account age indicator</b>	Optional	<p>Length of time that the cardholder has had the account with the 3DS requestor</p> <p>The following values are accepted:</p> <ul style="list-style-type: none"> <li>• 01 = No account (guest checkout)</li> <li>• 02 = Created during this transaction</li> <li>• 03 = Less than 30 days</li> <li>• 04 = 30 to 60 days</li> <li>• 05 = More than 60 days</li> </ul>
<b>Cardholder account change indicator</b>	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
<b>Delivery time frame</b>	Optional	Indicates the merchandise delivery time frame
<b>Gift card amount</b>	Optional	For prepaid or gift card purchase, the purchase amount total of prepaid or gift card(s)

Data element	Required?	Definition
<b>Merchant category code</b>	Required (for payment transactions)	Specific code describing the merchant's type of business, product, or service
<b>Shipping indicator</b>	Optional	<p>Indicates shipping method chosen for the transaction</p> <p>Merchants must choose the shipping indicator code that most reasonably and fairly describes the cardholder's specific transaction, not its general business. Examples include the following:</p> <ul style="list-style-type: none"> <li>• 01 = Ship to cardholder's billing address</li> <li>• 02 = Ship to another verified address on file with merchant</li> <li>• 03 = Ship to address that is different than the cardholder's billing address</li> <li>• 04 = "Ship to store"/pick up at local store (store address shall be populated in shipping address fields)</li> <li>• 05 = Digital goods (includes online services, electronic gift cards, and redemption codes)</li> <li>• 06 = Travel and event tickets, not shipped</li> <li>• 07 = Other</li> </ul>

Source: Aite Group, EMVCo

The enriched dataset has the potential to provide a significant performance boost in fraud management while also improving the customer experience. 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 behaviour but have no way to share those insights to help inform the issuer's authorisation and authentication decisions.

EMV 3DS finally provides the mechanism for merchants to share this data with issuers to reduce false declines while also better detecting fraud. In the U.K., for instance, CNP fraud accounts for about 75% of all card fraud but is starting to decline due to high issuer adoption of 3DS. With the introduction of EMV 3DS, this trend looks set to continue due to the increased levels of protection and data available for issuers to authenticate and make decisions regarding their cardholder transactions.

## EMV 3DS BENEFITS

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

- **Regulatory compliance:** In response to rising fraud, the EBA and the card networks have mandated the use of multifactor authentication for e-commerce transactions. EMV 3DS provides compliance with these mandates, as described in Table B.
- **Mitigation of fraud liability exposure:** As with 3DS 1.0, if a merchant uses EMV 3DS then the liability for fraud seen through this channel rests with the issuer. This increase in net loss exposure will be compounded for issuers not enabled for EMV 3DS.
- **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. This also translates to reduced costs as chargebacks decline, and the contact centre has fewer inbound calls related to CNP fraud and false declines.

**Table B: Multifactor Authentication Mandates in Europe**

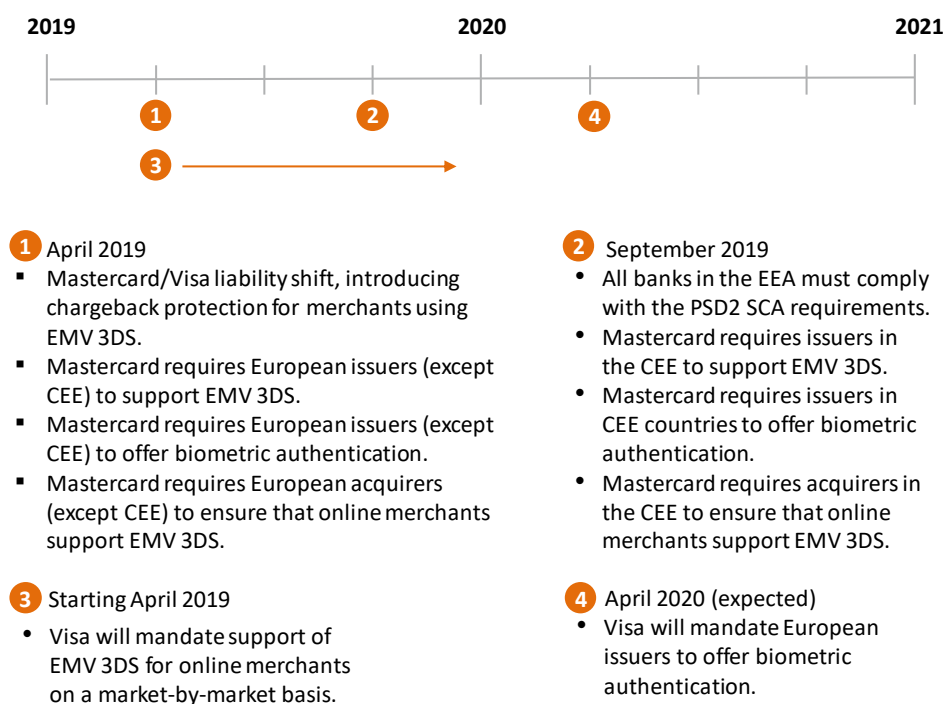
Mandating entities	Description
<b>EBA</b>	PSD2 mandates SCA to be implemented for electronic transactions in the European Economic Area (EEA) by September 2019. Payment service providers (PSPs), which include banks, e-money providers, and payment institutions, must apply SCA for all electronic payments 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.
<b>Mastercard</b>	<p>Mastercard requires European issuers to support EMV 3DS by April 2019 (Central and Eastern Europe [CEE] by September 2019) on e-commerce transactions.</p> <p>Mastercard is mandating that issuers offer their customers biometric authentication for Mastercard Identity Check/SecureCode and Masterpass transactions, including near-field communication (NFC) mobile transactions. Issuers will have to offer an alternative authentication method for cardholders without a smartphone (e.g., an OTP via SMS).</p> <p>Mastercard requires European acquirers to ensure that online merchants support EMV 3DS by April 2019 (CEE by September 2019).</p> <p>SCA must be based over time on non-static authentication.</p> <p>3DS is also required for all online gaming transactions.</p>

Mandating entities	Description
<b>Visa</b>	<p>Issuers that submit secure e-commerce transactions must support Verified by Visa.</p> <p>Merchant liability protection for EMV 3DS will apply from April 2019. Mandates for merchants to migrate to EMV 3DS will be announced on a market-by-market basis.</p> <p>Issuers must support a Visa-recognised payment authentication method. The support of biometrics will be mandated by Visa.</p> <p>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.</p>

Source: Aite Group, Visa, Mastercard

The mandates are summarized in Figure 6.

**Figure 6: EMV 3DS European Milestone Dates**

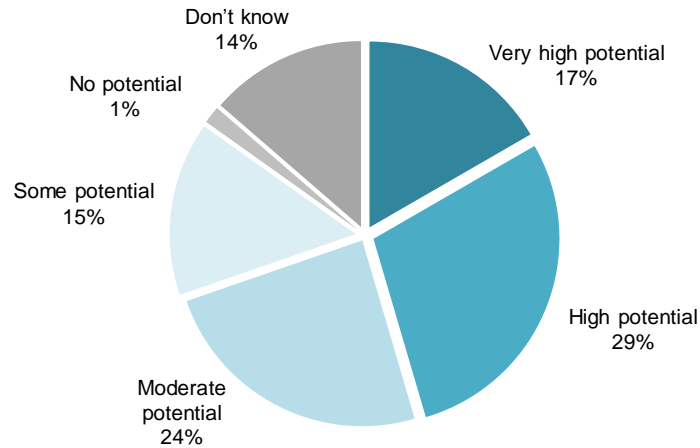


Source: EBA, Mastercard, Visa, Aite Group

Although live data are not yet available, the market recognises the promise of EMV 3DS. Recent research by Aite Group and Mobey Forum shows that almost half of payment executives view EMV 3DS as having high or very high potential to provide a better balance between security and a frictionless payment experience (Figure 7).

**Figure 7: Market Assessment of EMV 3DS**

**Q. How much potential do you see in EMV 3-D Secure to provide a better balance than the original 3-D Secure between proper security and frictionless user experience in m-commerce payments?**  
(n=66)



Source: Aite Group and Mobey Forum online survey with 76 executives, November 2017

## PSD2 STRONG CUSTOMER AUTHENTICATION REQUIREMENT

Effective September 2019, PSD2 mandates SCA for the initiation of electronic payments, including (but not limited to) e-commerce transactions. For card payments, SCA requires the issuer to invoke multifactor authentication of its customer. SCA must be based on at least two of the following independent factors that identify the cardholder:

- **Knowledge:** This is something only the customer knows, which may be a password or PIN. Note that recent guidance by the EBA does not consider card data (e.g., card number, CVV, or expiry date) as a knowledge factor.<sup>5</sup>
- **Possession:** This is something the customer has—for example, a smartphone or hardware token.
- **Inherence:** This is something the customer “is,” e.g., a biometric factor such as fingerprint or facial recognition. Behavioural biometrics is also recognised by the EBA as a valid inherence factor.

SCA will have significant impact in particular for e-commerce transactions. Consumers will face many more stepped-up authentication requests, exposing merchants to the risk of cart abandonment and loss of sales. Fortunately, not all transactions will require SCA, as the regulation specifies a number of exemptions that qualify as “low-risk” transactions, as follows:

5. “Opinion of the European Banking Authority on the Implementation of the RTS on SCA and CSC,” EBA, June 2018, accessed 24 September 2018, <https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf/0f525dc7-0f97-4be7-9ad7-800723365b8e>.

- Transactions that are under 30 euro 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 organised crime rings test stolen cards with low-value transactions. This exemption also doesn't help much for merchants that sell goods at an average transaction value well above the threshold, such as fashion or electronics.
- Not all transactions under 30 euro will go unchallenged, as there are cumulative limits in place that require SCA when these limits are reached. Issuers have the choice to either challenge every fifth transaction (below 30 euro), or request SCA if the combined value of several unchallenged transactions goes above 100 euro. This could present some difficulty for merchants that will have to deal with customers' expectations of a frictionless process.
- The customer can whitelist trusted merchants. Whitelisting is a vital tool for merchants that offer card-on-file or wallet payment options (card-on-file payment volume constitutes about one-third of all online payments). The request to whitelist the merchant can be offered to the customer with the first payment. SCA is required for the customer's first payment to the business but not for subsequent payments, with no limit to transaction amount.

Whitelisting can only be done under the control of the issuer (not by the merchant or the acquirer). Issuers should limit whitelisting to low-risk merchants (e.g., based on merchant category code and fraud rates), and monitor traffic for whitelisted merchants to detect risk indicators, such as a change of delivery address. In such cases, issuers should invoke SCA.

- PSPs can make use of the exemption for transaction risk analysis (TRA). TRA allows PSPs to apply risk-based authentication and choose not to apply SCA. The TRA exemption sets a threshold that depends on the fraud rates of the PSP applying the exemption:
    - If the fraud rate is below 13 basis points, there is no requirement for stepped-up authentication for transactions of up to 100 euro. If the fraud rate is below 6 basis points, that ceiling rises to 250 euro. For those with a rate of under 1 basis point, only transactions over 500 euro require stepped-up authentication.
- The fraud rate for the application of the TRA exemption is calculated as the total value of unauthorised and fraudulent remote card transactions divided by the total value of all remote card transactions. This must be calculated for all card payments processed by the PSP within the EEA.
- TRA can be applied by the acquirer (not by the merchant) or by the issuer. If the acquirer uses the TRA exemption, it will be liable for the payment in case of fraud.
  - 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 euro, it will need to be challenged.

Issuers are strongly recommended to implement the exemptions given above, in particular the whitelisting and TRA exemptions.

The EMV 3DS specification provides the framework for issuers to implement the SCA requirements. It also enables issuers to make more informed decisions based on data provided by merchants and acquirers, and it mitigates the risk of a deterioration of the consumer experience in e-commerce due to the PSD2 SCA requirement.

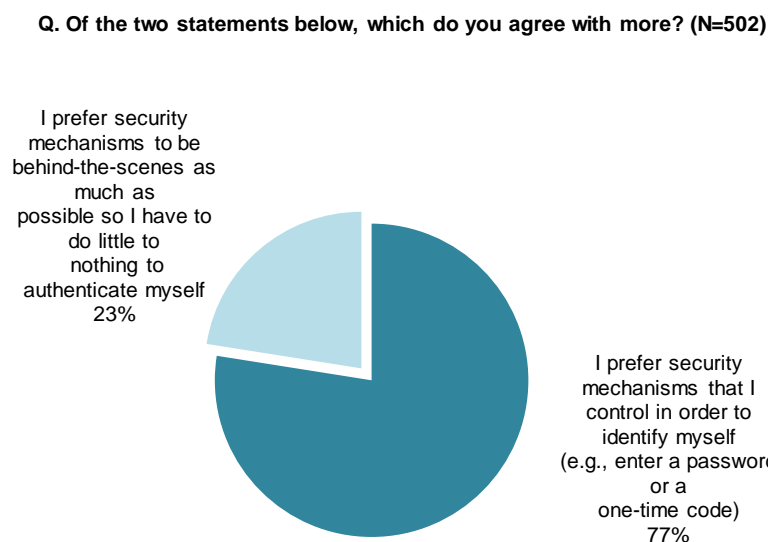
European issuers report that around 20-25% of their e-commerce transactions travel along the 3DS protocol (representing around 50% of the value of these transactions). Many issuers and payment network executives expect to see this increase to well above 90% with the PSD2 requirement for SCA.

## THE PATH FORWARD: BETTER SECURITY, FEWER FALSE DECLINES

As the industry enables EMV 3DS, the new standard can help improve CNP transaction performance on several fronts. EMV 3DS has the potential to reduce false declines, increase authorisations, and reduce fraud. And 3DS provides a clear path to PSD2 compliance.

Gone are the days when fraud was a topic that could be swept under the rug. 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 8.

**Figure 8: Consumers' Attitudes Toward Control Over Authentication Mechanisms**



Source: Aite Group survey of 502 consumers in the U.K., July 2018

A key question for most issuers is what kind of performance benefits they can expect to reap. While no EMV 3DS performance data exist yet, as the protocol is new, the earlier version, 3DS 1.0.2, also supports a risk-based authentication approach and can provide some informative leading indicators, as detailed below. These metrics should only improve as merchants send through the enriched data stream available with EMV 3DS, which should result in better issuer decisioning. Issuers can also fully leverage the new wealth of additional data sources.

- **Authorisations:** According to one of the payment schemes, 3DS transactions generally see 10% to 11% higher authorisation rates than non-3DS transactions in markets with widespread 3DS use. A large travel merchant in the U.S. (a market with limited 3DS use) that has deployed 3DS for the bulk of its volume says that it has seen a 2.4% increase in authorisations compared to its pre-3DS authorisation rates. The increase in authorization rates implies a commensurate decrease in false declines.
- **Stepped-up authentication rate:** Prior Aite Group studies have shown an average stepped-up authentication rate of 5% among issuers using the version 1.0.2's risk-based authentication capabilities.<sup>6</sup> This rate will likely decrease with the enhanced data stream from EMV 3DS.

---

6. 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 comply with the PSD2 SCA mandate, while also providing a vastly improved customer experience compared to 3DS 1.0. There is urgency for issuers to migrate to EMV 3DS to be ready and avoid chargeback losses when the liability shift kicks in by April 2019. Here are some recommendations for issuers as they are planning enablement of EMV 3DS:

- **Look for a partner well-versed in the nuances of 3DS.** Issuers should look for a partner 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 can help maximise detection and minimise false declines.
- **Prioritise feeding the data into your authorisation system.** The enriched data flow will not only help improve authentication rates but will also help with authorisation. It's understandable that issuers will want to walk before they run, but feeding data to the authorisation routines should be on the roadmap for all issuers to maximise 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.
- **Implement the PSD2 exemptions,** in particular the whitelisting and TRA exemptions. These exemptions are vital for online merchants to continue to offer frictionless one-click payments and minimise the impact of the PSD2 SCA regulation for cardholders and merchants.

## 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

**Ron van Wezel**

+31.6.3629.6515

[rvanwezel@aitegroup.com](mailto:rvanwezel@aitegroup.com)

## CONTACT

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

**Aite Group Sales**

+1.617.338.6050

[sales@aitegroup.com](mailto:sales@aitegroup.com)

For all press and conference inquiries, please contact:

**Aite Group PR**

+1.617.398.5048

[pr@aitegroup.com](mailto:pr@aitegroup.com)

For all other inquiries, please contact:

[info@aitegroup.com](mailto: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/issuers](https://ca.com/issuers).

## ABOUT TSYS

TSYS (NYSE: TSS) is a leading global payments provider, offering seamless, secure and innovative solutions across the payments spectrum for issuers, merchants, and consumers. We succeed because we put people and their needs at the heart of every decision to help them unlock payment opportunities. It's an approach we call People-Centered Payments.

Our headquarters are located in Columbus, Georgia, with approximately 12,000 team members and local offices across 13 countries. TSYS generated revenue of US\$4.9 billion in 2017, while processing more than 27.8 billion transactions. We are a member of The Civic 50 and were named one of the 2018 World's Most Ethical Companies by Ethisphere Magazine. TSYS is a member of the S&P 500 and routinely posts all important information on its website, [tsys.com](https://www.tsys.com). For more information on the array of risk and fraud tools and services that TSYS offers European issuers, contact [sales@tsys.com](mailto:sales@tsys.com).