Carat

Understanding and preparing for the impact of PSD2

Just as “no man is an island,” the success of a company does not stand on a single person.

This is especially true with Carat, where every employee is considered an “owner-associate.”

This not only gives them a stake in the company, but also makes everyone accountable for company growth. Thankfully, the collective expertise of our team supports our ability to innovate and deliver solutions that help drive the new world of global digital commerce.

Executive Summary

Understanding and preparing for the impact of PSD2

PSD2 is the revised Payment Services Directive enacted by the European Commission (EC) on January 13, 2018. It is scheduled to take full effect on September 14, 2019, at which time providers will need to implement the technical requirements, including Strong Customer Authentication (SCA), outlined in PSD2.

Its mandates are far-reaching, affecting not only enterprises within the European Union but also any online retailer with European customers. In fact, to increase security for remote transactions in their own countries, many non-EU governments have adopted some of the mandates first proposed by the EC.

So, no matter where our clients conduct their business, it's critical they have a working understanding of PSD2, its provisions and some of the solutions that can help make compliance possible.

It's our hope that by going through this material and understanding its content, our clients will be better prepared for the changes ahead.

As always, First Data stands ready to help our customers navigate new revenue streams that are safer and that have greater potential than ever before. This is just the beginning of our lasting journey together.

Objectives

- Explore the Origins of PSD2, what it was designed to do, its drivers and key provisions, important dates and its effect on established players and on new entrants in the market
- Explain Strong Customer Authentication, as a key component of PSD2 and as an increasingly widespread mandate for countries around the world
- Look at EMV 3-D Secure, a leading solution designed to satisfy the SCA mandate and helps make online transactions safer and more frictionless compared to its previous version

Part I:

What is PSD2?

The revised Directive on Payment Services, known as PSD2, is a mandate that governs regulated payment service providers within the European Union and the European Economic Area. It is designed to increase competition and participation in the European payments system for merchants and other stakeholders.

When does it apply?

All electronic payment transactions where either the buyer or the seller uses an EU-based regulated payment service provider are potentially subject to PSD2 mandates.[1]

What are the key dates?

PSD2 has been in place since January 13, 2018. However, it won't come into full effect until September 14, 2019, which is the deadline for providers to comply with PSD2s technical requirements, including Strong Customer Authentication.[2] (See Section Two).

Background

In seeking to create more competition for digital transactions and ultimately, better services for European customers, the EC in 2012 published a Green Paper entitled "Towards an integrated European market for card, internet and mobile payments."[3]

"We have already used EU competition rules to ensure that new and innovative players can compete for digital payment services alongside banks and other traditional providers. The new Directive will greatly benefit European consumers by making it easier to shop online and enabling new services to enter the market to manage their bank accounts."[4]

Margrethe Vestager,
European Commissioner for Competition

To that end, the EC has identified four main PSD2 drivers and their benefits:[5]

More competition

More choice and transparency for the consumer

More innovation

More payment security and customer trust

More competition

The EC wants to lessen the dominance of American card schemes Visa® and Mastercard®, which are used in nearly 87 percent of global transactions.[6] It hopes that by adopting open standards, providers would offer their payments solutions in more than one country, giving rise to increased competition.

More choice and transparency for the consumer

Previously, electronic payment transactions were controlled by a relatively small number of larger providers – mainly banks – who often had hidden costs and limited services.

PSD2 is designed to open access to customers' bank accounts to third-party providers who can debit and credit those accounts directly. With better insights into what they are getting and associated cost, it's hoped that customers will choose providers with the best rates and services.

More innovation

The EC is looking to drive down the cost of entry and is encouraging innovative companies to test the market with new products.

With full EU-wide scale now possible, innovations by new or existing companies will likely be rewarded more quickly.

More payment security and customer trust

Seeking to replicate the success of EMV® card chips, which reduced fraud at the point-of-sale (POS), the EC is now mandating new safeguards to protect remote transactions.

The EC hopes these safeguards will boost consumer confidence in electronic and mobile payments, and subsequently increase online vendor revenue.

Up to

87%

of global transactions used Visa and Mastercard[vi]

Key provisions:

1. **Give Third-Party Payment Providers (TPP) access to payment accounts.** Banks must grant TPPs access to consumer's payment accounts (XS2A).[7] Two new types of TPPs have been defined:
   a. **Account Information Service Providers (AISP)** – AISPs offer online services which can provide a consolidated view of a consumer's payment accounts.
   b. **Payment Initiation Service Providers (PISP)** – PISPs initiate payment transactions at the request of the consumer from an account held by the consumer at another payment service provider.
2. **Introduce Strong Customer Authentication (SCA).** Subject to certain exemptions, SCA is mandated for electronic payment transactions and requires authentication by two or more independent factors.
3. **Reduce consumer liability.** Excluding fraud or gross negligence, a consumer's maximum liability for an unauthorized transaction is reduced from €150 to €50.[8]
4. **Prohibit surcharging on card payments.** Surcharges must not be applied to any transaction made with a consumer card that is accepted in accordance with the European Union's regulation on interchange fees for card-based payment transactions.[9]

What effect will PSD2 have on incumbents?

Banks: Face increased competition from AISPs and PISPs and a loss in issuing and payments revenue potentially offset by cost reductions. Banks can monetize data made available through open APIs and offer third-party products and services or become a PISP or AISP.

Card Schemes: Face revenue and market share erosion. Card schemes can diversify by becoming PISPs or AISPs.

Merchants: Will have more choice for payments, but will need to make investments for enablement and there could be a potential conversion rate drop-off due to SCA.

Payment Processors: Face increased competition from AISPs and PISPs and the cost of enabling bank account payments, but they can also become AISPs and PISPs.

PSPs and Acquirers: Face increased competition from AISPs and PISPs, bear the cost of enabling bank account payments and revenue and market share erosion, but they can also become AISPs and PISPs.

What effect will PSD2 have on new players?

PSD2 and the drive for third-party access to accounts and open banking standards provide opportunities for new entrants to the payments market, including:

AISPs: Will be able to offer value-added services such as data aggregation, identity verification and data analytics.

PISPs: Will be able to initiate payments without using a card network, helping to reduce cost latency and friction.

Part II:

What is SCA?

SCA stands for Strong Customer Authentication. It is a key mandate included in the PSD2 within the European Economic Area (EEA) that requires electronic payments initiated by the buyer to be authenticated by at least two independent factors. The European Union (EU) passed the SCA mandate to ensure electronic payment methods are carried out in a secure manner with as little fraud as possible. The EU believes the changes will create a trusted environment in which consumer spending will grow and payment innovations will thrive. The European Parliament believes SCA will lead to healthy, sustained economic growth for the entire region.

To whom does SCA apply?

- SCA applies only to non-exempt[1] electronic transactions that occur entirely within the EU/EEA. This means the card issuer and the merchant/acquirer are in the EEA
- For merchants located outside the EEA, SCA applies only on a best-effort basis. However, if a non-EEA merchant does not use SCA, they will be liable for any fraudulent transactions
- If a merchant is located within the EEA, but the consumer is using a card issued outside the EEA, SCA does not apply[3,4]

What are the key dates?

September 14, 2019, is the deadline for providers to comply with the SCA technical requirements.[5]

Background

With the accelerated growth of electronic payments, European authorities recognized that to have a healthy economy, they would need to protect remote payments. SCA grew out of this need to protect electronic payment transactions, including E-payments (online/internet) and M-payments (mobile devices), with similar protections afforded to in-person transactions using EMV chips. Some examples of these types of transactions include the following:[5]

- Online payment account services, such as balance inquiry, review of statements, whitelisting of trusted beneficiaries or block beneficiaries
- Initiation of electronic payments, such as card payments, credit transfers, e-money transactions and direct debits

Two-Factor Authentication

The main requirement of SCA is that all non-exempt and customer-initiated electronic payments are authenticated using at least two of the three specified independent factors. The factors are deemed "independent" when they are derived from discrete sources, defined as follows:

Something you know

Password
Passphrase
PIN
Sequence
Secret Fact

Something you possess

Mobile Phone
Wearable Device
Smart Card
Token
Badge

Something you are

Fingerprint
Facial Features
Voice Patterns
Iris Format
DNA Signature

For SCA, the factors can be either two of these independent elements or something that works only when all the elements have been provided (for example, an algorithm in a chip produces a one-time password or cryptogram, based on a response to a PIN request).[6]

Additional Risk-Based Factors

Payment Service Providers (PSPs) are responsible for the application of SCA to applicable transactions and they must ensure that the transaction-monitoring mechanisms consider, at a minimum, each of the following risk-based factors.

Risk-based authentication is the evaluation of a transaction's risk profile that typically involves analyzing:

- Contextual data from the payee
- Payer/Payee transaction history
- Transaction characteristics, such as amount, device ID and location

---

A risk score model and/or risk rules can be used to determine if:

- Authentication is successful
- Additional payer information is required
- Authentication failed

Risk-based authentication allows issuers to authenticate their payers without asking for any additional information for the majority of transactions, performing step-up authentication only for the riskiest transactions. When used effectively, risk-based authentication can provide protection against fraud, increase completed sales and lead to a better experience for all stakeholders.

Under PSD2 SCA, PSPs must ensure for authenticated electronic payments that the transaction-monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:

- Lists of compromised or stolen authentication elements
- The amount of each payment transaction
- Known fraud scenarios in the provision of payment services
- Signs of malware infection in any sessions of the authentication procedure

---

Where PSPs allow the consumer to utilize SCA exemptions, they must ensure that the transaction-monitoring mechanisms take into account, at a minimum and on a real-time basis, each of the following risk-based factors:

- The previous spending patterns of the individual payment service user
- The payment transaction history of each of the payment service provider's payment service users
- The location of the payer and of the payee at the time of the payment transaction providing the access device or the software is provided by the payment service provider
- The abnormal behavioral payment patterns of the payment service user in relation to the payment transaction history
- In case the access device or the software is provided by the payment service provider
- A log of the use of the access device or the software provided to the payment service user and abnormal use of the access device or the software

Dynamic Linking

Each authentication event for a remote electronic payment must also be linked to a specific amount and a specific merchant, in a process known as Dynamic Linking.

PSD2 SCA Dynamic Linking requirements can be summarized as follows:

1. The consumer must be made aware of the merchant details and the payment amount when asked by the issuer to authenticate.
2. The authentication code generated by the issuer can be used only once and must be linked to the same merchant and amount as displayed to the consumer.
3. The authentication code must successfully authenticate only the electronic payment linked to the specific consumer and amount.
4. The resulting authentication code must be passed in the authorization request and must be unique for that specific electronic payment.
5. The issuer must validate that the authentication code passed in authorization matches the merchant and the payment amount of the authentication (bringing it back to number one).

Strong Customer Authentication (SCA) Requirements

Dynamic Link

Out of Scope

Several limited categories of transactions are out of scope of the SCA mandates.

#	Electronic Payment Category	Description
1	Direct Debits	Under PSD2, customers can give consent for third-party PSPs or specific merchants to initiate direct payments from their accounts. Because these transactions are not initiated by the customer, they are out of scope.
2	Payee/ Merchant Initiated Transactions	Similarly, customers can set up repeatable transactions, for instance, with streaming media or other digital services. These transactions are initiated by the merchant, not the customer and therefore, are out of scope.
3	Mail Order Telephone Order (MOTO)	Payments transacted over the phone are not considered to be electronic payments and therefore, are deemed out of scope for SCA.
4	Anonymous Payment Instrument Transactions	With transactions where anonymous prepaid cards are used, two-factor authentication is impractical, as it would require the cardholder to preregister the independent factors before making purchases. Therefore, these transactions are deemed out of scope.
5	Non-EEA Payments	SCA applies only to transactions made entirely within the EEA, governed by the European Banking Authority. Therefore, if either issuer or the acquirer is domiciled outside the EEA, no SCA mandates apply.[2]

Exemptions

The European Commission (EC) has taken steps to ensure merchants are not unduly burdened by the SCA mandate, setting aside certain transactions as exempt. Depending on the exemption, it is the responsibility of the merchant or acquirer to request an exemption. However, the issuer makes the final determination of exemption eligibility.[7]

#	Electronic Payment Category	Description	Merchant Qualifying Exemption	Consumer Use Cases
1	Low value (Article 16)	Electronic payments under €30 – and: • The cumulative amount of previous electronic payment transactions since the last application of SCA does not exceed €100; or • The number of previous electronic payments since the last application of SCA does not exceed five consecutive individual transactions	Yes	Niamh, who lives in Ireland, is almost out of shampoo and wants to order some online from her favorite salon in Paris. Because the payment is less than €30 and she has not initiated five consecutive unauthenticated transactions, she will not need to authenticate her payment.
2	Subscription or recurring transactions with a fixed amount (Article 14)	Payer-initiated recurring payments for the same amount, to the same payee, such as with digital subscription services. SCA is required for the payer's first transaction. Subsequent payments are exempt.	Yes	For the next three months, James will be traveling across Europe and wants to be able to stream new music as he explores. He signs up for a subscription music service that pulls funds from his account at the start of each month. He authenticates the first payment, but won't have to worry about it for the rest of his travels.
3	Trusted beneficiaries (Whitelisted payees/merchants) (Article 13)	Payers can assign payees to a whitelist of trusted beneficiaries that is maintained by their bank. Whitelisted payees are exempt from SCA.	No	Every other week, Anne orders dinner from her grandchildren's favorite takeout restaurant online and has it delivered. So that she does not need to authenticate each time, she lets her bank know that this is a trusted merchant.
4	Secure corporate payments (Article 17)	Electronic payments made through dedicated corporate processes initiated by businesses and not available to consumers. These payments include payments made through central travel accounts, lodged cards, virtual cards and secure corporate cards.	N/A	Phillip is a marketing director and received an invoice from one of his vendors for recently completed work. Because of the process instituted by his company, he does not need to authenticate the transaction.
5	Contactless payments (Article 11)	The value of the electronic payment through a mobile or contactless device at point-of-sale must not exceed €50 – and: • The cumulative limit of consecutive contactless transactions without application of SCA must not exceed €150; or • The number of consecutive contactless transactions since the last application of SCA must not exceed five	Yes	Heidi has found the perfect dress for her date this weekend for €45. Because the only other thing she has bought since her last authentication was a pair of shoes for €60, she will not need to authenticate the transaction for her new dress.
6	Unattended transportation and parking terminals (Article 12)	Electronic payments through unattended terminals for transportation fares and parking fees.	Yes	To take the train out to the beach on the weekend, Harry uses the kiosk to add more funds to his digital train ticket. Because it is an unattended terminal, he will not need to authenticate the transaction.

<table>
<tr><th>#</th><th>Electronic Payment Category</th><th>Description</th><th>Merchant Qualifying Exemption</th><th>Consumer Use Cases</th></tr>
<tr><td>7</td><td>Credit transfers between the same natural or legal person (Article 15)</td><td>Payment service providers shall be allowed not to apply SCA when a payer transfers funds between the payer’s own accounts serviced by the same payment service provider.</td><td>N/A</td><td>Suzanne transferred money from one of her accounts to another one of her accounts at the same bank. Because she is electronically moving money between accounts she owns, she does not need to authenticate the transaction.</td></tr>
<tr><td>8</td><td>Low-risk transactions/ transaction risk analysis (TRA) (Article 18)</td><td>A PSP will be allowed to do a real-time risk analysis to determine whether to apply SCA to a transaction. This is possible only if the PSPs fraud rates do not exceed the following thresholds:<table><tr><th>PSP Fraud Rate Threshold</th><th>Electronic Payment Exemption bands</th></tr><tr><td>13 bps/0.13%</td><td>Up to €100</td></tr><tr><td>6 bps/0.06%</td><td>€100 – 250</td></tr><tr><td>1 bps/0.01%</td><td>€250 – 500</td></tr></table></td><td>Yes</td><td>Thomas, who lives in Portugal, would like to order a new watch online from Switzerland for CHF225; converted, it is €200. Little does he know, but because the PSP used by the watch maker has such a low fraud rate (0.05 percent) behind the scenes, the PSP is able to instantly score Thomas as low-risk: He buys a lot of watches. That means Thomas does not need to authenticate the transaction.</td></tr>
<tr><td>9</td><td>Access to payment account information (Article 10)</td><td>To be able to access balances and historic payment transactions, consumers need to authenticate their account every 90 days. SCA is applied across web or apps.</td><td>N/A</td><td>Ellie checks her bank account balance once a week. Because she authenticated her account last week, she does not need to authenticate again this week.[8]</td></tr>
</table>

Note: The European banking Authority (EBA) requires the fraud rate to be assessed at the PSP level, as the fraud rate cannot be assessed on an individual basis for a specific merchant. If an electronic payment under TRA is in a non-Euro currency, a currency conversion must be applied to determine whether the payment qualifies.

What’s Next?

It’s important to note that although the SCA mandate goes into effect on September 14, 2019, many other countries outside the EU have adopted or will soon adopt, the SCA mandate. SCA continues to grow in importance and irrespective of specific geographic markets, a merchant solution for SCA is critical.

> “Carat's goal is to help you drive revenue by enabling commerce.”

Part III:

EMV 3-D Secure

The European Commission (EC) has established new mandates under its Revised Payment Service Directive, known as PSD2. The open banking reforms allow third parties to access customer financial accounts in Europe for use in payment services.

PSD2 also seeks to protect customers who make transactions online or over mobile devices. For this, the European Commission established mandates for Strong Customer Authentication (SCA), which, among other requirements, ensure that eCommerce transactions are authenticated using at least two independent identifiers unless exemptions apply.

What is EMV 3-D Secure?

When the European Commission originally envisioned Strong Customer Authentication, the EC decided against establishing specific universal protocols that would securely enable online transactions and meet the requirements of the PSD2 SCA mandate. This decision led to some confusion among merchants eager to take advantage of secure transactions but unsure which protocols to use.

The major global payment networks had their own branded products that used a common protocol to authenticate purchases across three domains (3-D), the acquiring bank, issuing bank and interoperability protocol, which together made up 3-D Secure.

With the advent of the SCA mandate and the absence of standard protocols, Visa, Mastercard and other card companies within the global standards body, EMVCo (the same body that created protocols for EMV chips in credit and debit cards), established new online standards they incorporated into an updated product called EMV 3-D Secure. These protocols were quickly recognized by the EC as the de facto standards for the SCA mandate.

Do Merchants Have to Register?

Yes. Merchants should check with their acquirers to ensure they are ready for PSD2 SCA when the mandate goes into effect.

What are the Key Dates?

The payments industry is transitioning from 3-D Secure 1.0, using a gradual, European Union (EU)-wide regional rollout before the PSD2 SCA mandate's effective date of September 14, 2019. The 3-D Secure transition continued into 2020 for other geographic regions, so check with your processor for specific regions and products.

It is possible that some European Economic Area (EEA) Issuing Banks may only be able to support only 3-D Secure 1.0 after the September 14, 2019, SCA effective date. For this reason, global payment networks recommend payees and merchants that are already using 3-D Secure 1.0 continue to support that standard as well as introducing EMV 3-D Secure, until the payment networks' end-of-support timeline ends, that was expected to be somewhere between 2020 and 2021.

Is There a Liability Shift Associated with EMV 3-D Secure?

Yes. When a merchant begins using EMV 3-D Secure for authentication, provided that the liability shift date for the merchant's region is in effect, the merchant is no longer responsible for chargebacks due to fraud. For example, as a general rule, if a lost or stolen card is successfully used to complete a transaction where EMV 3-D Secure is in place, there is a liability shift from the merchant to the card issuer with respect to that transaction. If the issuing bank supports only 3-D Secure 1.0, the same liability shift occurs.

- The liability shift for Visa in Europe was April 2019
- The liability shift for Visa in the U.S. is August 2020
- The overall liability shift for Mastercard is October 2019

Otherwise, the activation dates for the liability shift are staggered by payment network and geography. Contact your acquirer for a full list of liability shifts and dates by region, product category and standards.

3-D Secure 1.0 and EMV 3-D Secure Co-Exist

According to the global payment networks, they envision the liability shift of 3-D Secure 1.0 will co-exist with the EMV 3-D Secure liability shift for a period of time.

This will allow merchants that are not yet upgraded to continue to use 3-D Secure 1.0. Issuers should not decline 1.0 transactions and issuers' Access Controlled Server (ACS) must be capable of handling 3-D Secure 1.0 and EMV 3-D Secure.

An Overview of EMV 3-D Secure

EMV 3-D Secure, sometimes called 3-D Secure 2.0, analyzes contextual and historical data using AI and machine learning tools to recognize expected purchasing patterns and to request additional prompts only on the riskiest transactions. Risk-based authentication is important in EMV 3-D Secure due to PSD2 SCA requirements and it involves analyzing the following:

- Contextual data from the payee
- Payer/payee transaction history
- Transaction characteristics such as amount, device ID and location

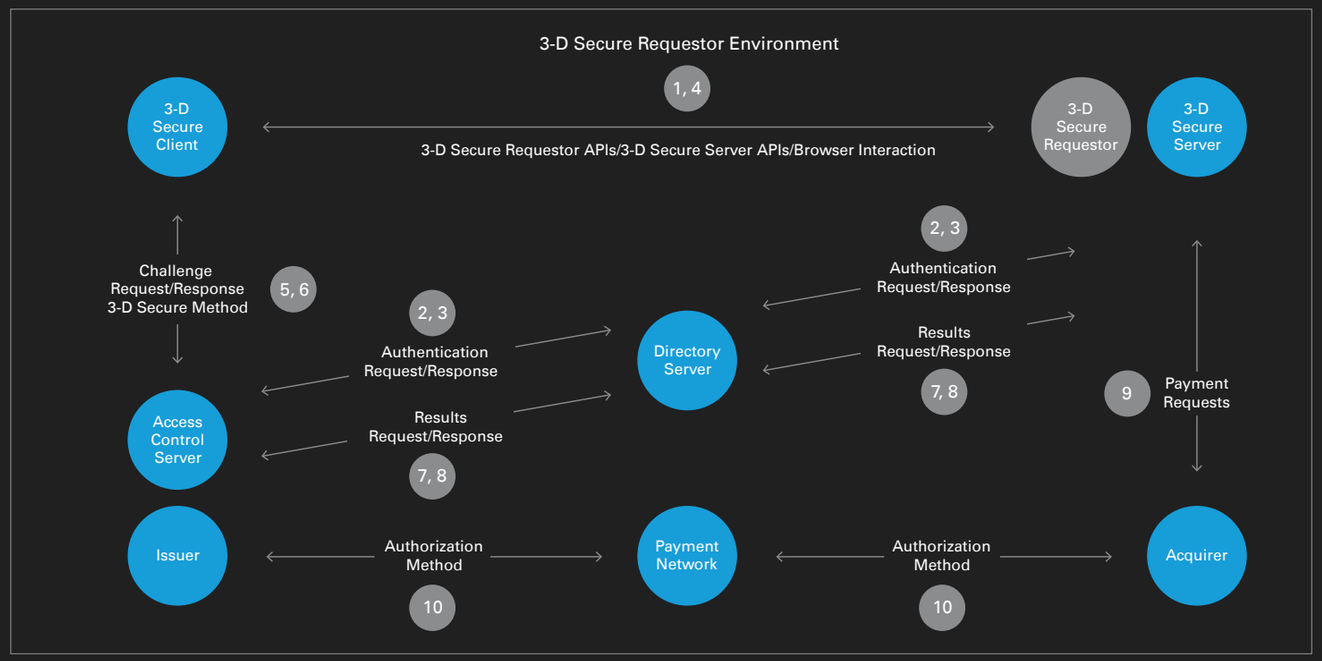
While the updated version of 3-D Secure responds to the PSD2 SCA mandate within the EEA, EMV 3-D Secure also impacts the security of online transactions globally, by making them more frictionless and reducing cart abandonment.

The previous version involved sending online purchases a series of prompts – security codes texted to phones or pop-up windows – which caused friction and apprehension about online payment safety. This led to increased frustration.

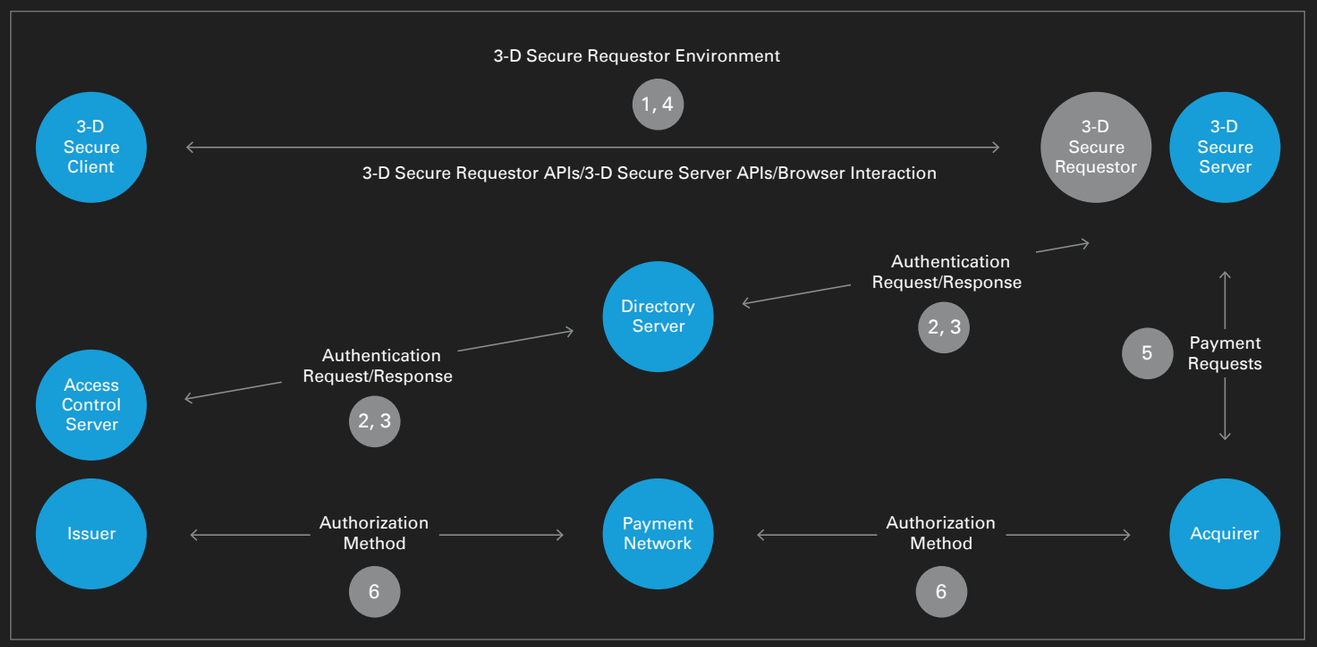
The update allows merchants or merchant acquirers to set their tolerance for authentication challenges, after assessing the authentication request and applying their own risk algorithms.

EMV 3-D Secure Authentication Flows[i]

Authentication Flow With Issuer Challenger



Authentication Flow



Updates from 3-D Secure 1.0 to EMV 3-D Secure

- Improved messaging with supplementary information for better decisions about authentication
- Non-payment user authentication
- Non-standard extensions to meet specific regulations and requirements, including proprietary out-of-band authentication solutions, used by card issuers
- Better performance for end-to-end message processing
- Improved data sets for risk-based authentication
- Prevention of unauthenticated payment, even if a cardholder's card number is stolen or cloned
- Enhanced functionality that enables merchants to integrate the authentication process into their checkout experiences, for app- and browser-based implementations
- Enables Merchant-initiated account verification
- Specific app-based purchases on mobile and other consumer devices supported

EMV 3-D Secure Authentication Standards Overview

Although EMV 3-D Secure is often referred to as 3-D Secure 2.0, there have been several standards updates and newer versions, all with improved functionalities built in.

EMV 3-D Secure

2.1

First-generation EMV standard

- Supports Strong Customer Authentication for connected devices and web purchases
- Supports non-payment authentication scenarios, such as payment card on-boarding to merchant apps

2.2

The standard contains specifications for handling the SCA exemptions and other Europe-specific scenarios in support of PSD2, such as trusted beneficiary and delegated authentication

One point of clarification is that MasterCard has extended their 2.1 specifications to support SCA exemptions

---

How to Use EMV 3-D Secure to Increase Revenue and Optimize the Customer Experience

Carat enables our clients to increase their revenues with the least amount of consumer friction possible, to reduce their costs through the maximum liability shift possible and to reduce the overhead by maintaining every client's current integration point for the enhanced EMV 3-D Secure service.

EMV 3-D Secure demands more transactional data, applying that information to contextual analysis which limits customer challenges, while keeping transactions safe. But, of course, you want to keep that data safe as well. Carat will manage this securely behind the scenes, to provide each client with a route out of the high cost of fraud, while minimizing the friction to each consumer to protect revenue.

We are working closely with regulators and payment programs to ensure that our services are PSD2 SCA compliant and that they can support all out-of-scope and exempt electronic payment categories, to ensure the best possible authorization outcomes for our merchants.

Carat offers three electronic payment services that are affected by PSD2 SCA:

- Gateway: Merchants using a Carat gateway can leverage our 3-D Secure solution as part of their gateway integration. The end-to-end readiness for EMV 3-D Secure should be validated with other components within the transaction flow, such as front and back-end systems

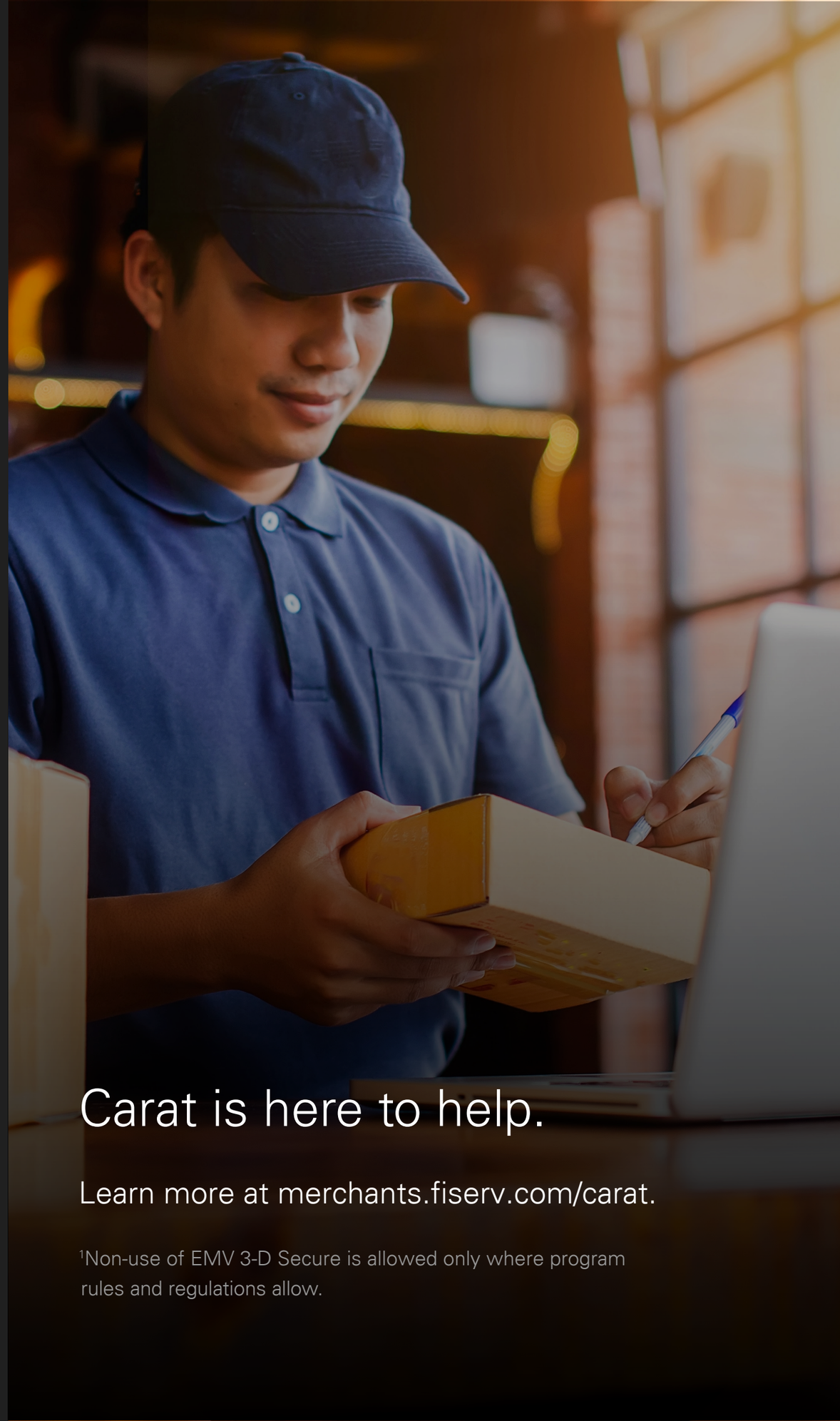
- **Acquiring:** Merchants that acquire with Carat will benefit from our full approach to SCA, including PSD2 scope management and SCA exemption management, if they also use our 3-D Secure solution
- **Processing:** Merchants who only process with Carat should consult with their acquirer (and their 3-D Services Provider for guidance for how SCA will be applied). Carat is evaluating its policies related to authentication data which will be received from third party payment services providers

What Should Merchants Do Today?

Merchants should evaluate the changes that are needed for their user interfaces, including mobile application flows. The management of out-of-scope transactions, transaction exemptions and chargeback liability shifts prevents a "one size fits all" implementation. Therefore, it is critical to make sure you understand how your current payment flows could be affected, when you want to utilize a 3-D Secure Solution and when you want to carry your own risks to provide the consumer experience that will deliver on your business goals in your digital strategy.[1]

Merchants should also look at the technical cost to enable a 3-D Secure Solution within their technical infrastructure. With incremental data requirements, merchants should work with their payments provider to understand whether their current integrations require refreshing and how to minimize the effort and cost of providing the solution the merchant needs in 2019.

Finally, merchants should understand their customer base, their business model and their current fraud rates to determine how a 3-D Secure Solution can benefit their digital business. The 3-D Secure Solution is a tool to enable both merchants and issuers to reduce their costs related to fraud, but there are still key decisions to be made to implement it in a way that does not negatively impact business goals.



Carat is here to help.

Learn more at merchants.fiserv.com/carat.

[1]Non-use of EMV 3-D Secure is allowed only where program rules and regulations allow.

Key Term Glossary

PSD2

Revised Directive on Payment Services

A mandate that governs regulated payment service providers within the European Union and the European Economic Area. It is designed to increase competition and participation in the European payments system for merchants and other stakeholders.

3DS

Three Domain Secure

The major global payment networks had their own branded products that used a common protocol to authenticate purchases across three domains (3-D): The acquiring bank, the issuing bank and an interoperability protocol, which taken together made up 3-D Secure.

EBA

European Banking Authority

An independent European Union Authority that help to maintain financial stability in the EU by managing European banking regulations.[1]

[1] eba.europa.eu/languages/home_en

[2] tripsavvy.com/countries-that-are-eea-countries-1626682

[3] firstdata.com/en_us/insights/emv-chip-card-technology.html

EEA

European Economic Area

The countries that are part of the EEA include Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latthrough, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.[2]

EMV

Europay Mastercard Visa

The chip card transactions improve protection against fraud when compared to traditional magnetic stripe credit cards. EMV can be used for credit and debit card transactions and most recently, NFC mobile payments. Unlike its predecessors, EMV-enabled cards use a smart chip, instead of a magnetic stripe, to hold the data required to complete a purchase.[3]

SCA

Strong Customer Authentication

A key mandate that's included in the PSD2 within the European Economic Area that requires electronic payments initiated by the buyer to be authenticated by at least two independent factors.[3]

Sources

Part I: What is PSD2?

[1] Payment Services Directive: frequently asked questions. European Commission. Jan 12, 2018. Question 8. europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en

[2] Payment Services Directive (PSD2): Regulatory Technical. Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments. European Commission. Nov. 27, 2017. Question 1. europa.eu/rapid/press-release_MEMO-17-4961_en.htm

[3] Towards an integrated European market for card, internet and mobile payments. European Commission. Nov. 4, 2012. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011DC0941

[4] European Parliament adopts European Commission proposal to create safer and more innovative European payments. European Commission. Oct. 8, 2015. europa.eu/rapid/press-release_IP-15-5792_en.htm

[5] Towards an integrated European market for card, internet and mobile payments, European Commission. Nov. 4, 2012. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011DC0941

[6] Visa versus Mastercard: Is There a Clear Winner? Grizzle.com. April 15, 2019. grizzle.com/visa-vs-mastercard/

[7] NextGen PSD2. A European Standard for PSD2 XS2A. The Berlin Group. docs.wixstatic.com/ugd/ c2914b_71cd1468acb24cc79e5476ef5bc033c3.pdf

[8] Payment Services Directive: frequently asked questions. European Commission. Jan. 12, 2018. europa.eu/rapid/press-release_MEMO-15-5793_en.htm

[9] Payment Services Directive: frequently asked questions. European Commission. Jan. 12, 2018. europa.eu/rapid/press-release_MEMO-15-5793_en.htm

---

Part II: What is SCA?

[1] Payment Services Directive: frequently asked questions. European Commission. Jan 12, 2018. Question 16. europa.eu/rapid/press-release_MEMO-15-5793_ en.htm?locale=en

[2] Directive (Eu) 2015/2366 of the European Parliament and of the Council. Official Journal of the European Union. Article 97. Dec 23, 2015. eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

[3] Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC. European Banking Authority. Jun 13, 2018. eba.europa.eu/documents/10180/2137845/Opinion+on+the+ implementation+of+the+ RTS+on+SCA+and+CSC+%28 EBA-2018-Op-04%29.pdf

[4] Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments. European Commission. Nov. 27, 2017. Question 1. europa.eu/rapid/press-release_MEMO-17-4961_en.htm

[5] Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2). European Banking Authority. Dec 8, 2015. eba.europa.eu/documents/10180/1303936/EBA-DP-2015-03+%28RTS+on+SCA+and+CSC+under+PSD2%29.pdf

[6] Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2). European Banking Authority. Dec 8, 2015. Item 31. eba.europa.eu/documents/10180/1303936/EBA-DP-2015-03+%28RTS+on+SCA+and+CSC+under+PSD2%29.pdf

[7] Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC. European Banking Authority. Jun 13, 2018. eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28 EBA-2018-Op-04%29.pdf

[8] Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC. European Banking Authority. Jun 13, 2018. eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28 EBA-2018-Op-04%29.pdf

---

Part III: EMV 3-D Secure

[1] PEMV® 3-D Secure Protocol and Core Functions Specification. EMVCo. Dec 2018. emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_v220_122018.pdf

fiserv.

Carat