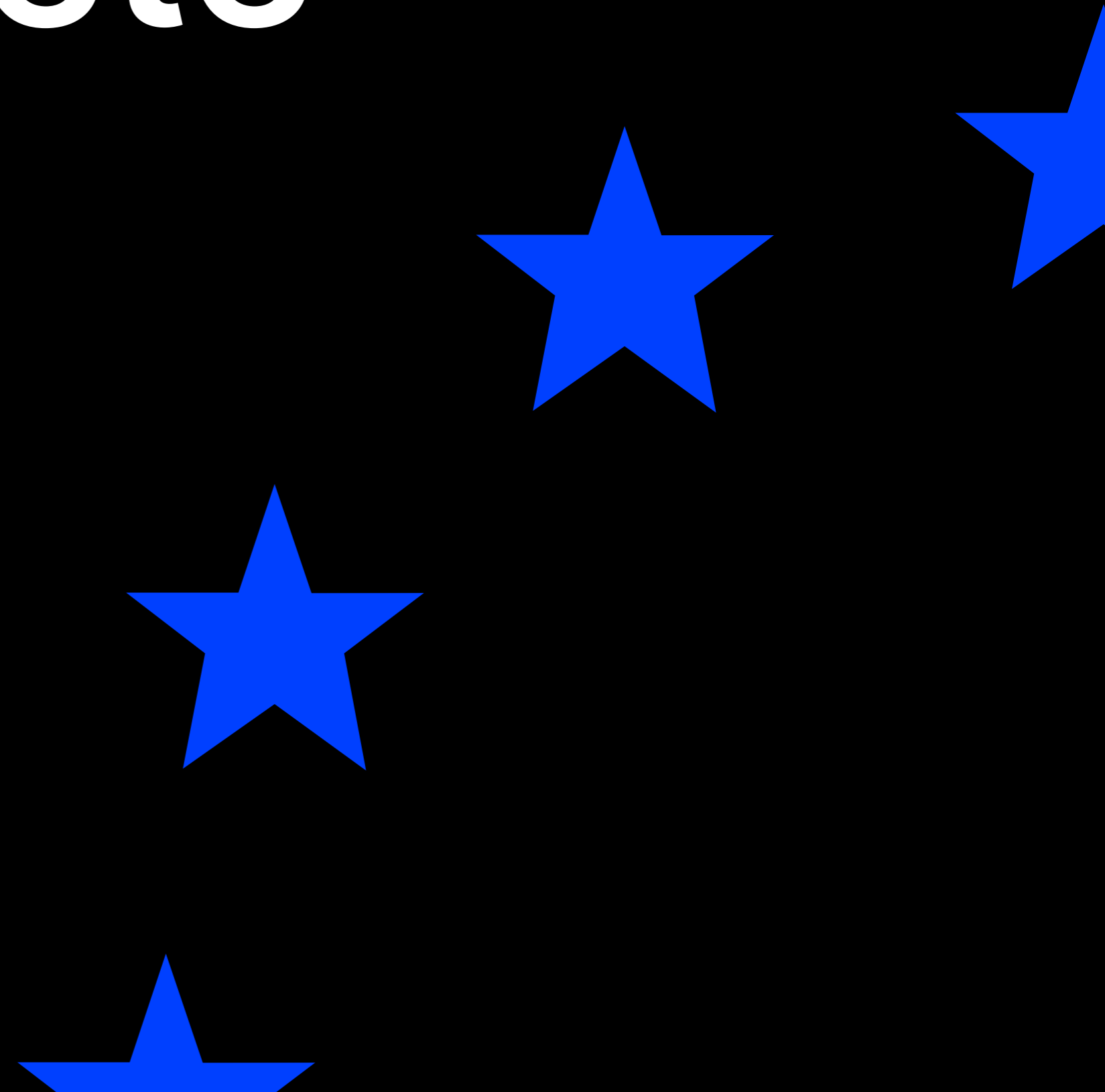


De e-commerce retailers' complete gids naar PSD2

mollie

Voorbereid zijn op Strong
Customer Authentication



Inhoud

- 3 Afkortingen
- 4 Wat betekent PSD2 voor jouw e-commerce bedrijf
- 5 Betalingen naar het digitale tijdperk brengen

Deel 1

7 **What is PSD2**

- 8 Waarom PSD2
- 9 Van PSD1 naar PSD2

Deel 2

14 **Het effect van PSD2 op merchants: Strong customer authentication**

- 15 Waarom strong customer authentication (SCA)
- 16 Hoe hebben merchants voordeel bij SCA
- 18 Hoe vraag je SCA-vrijstellingen aan
- 19 Wat is het effect van SCA op kaartbetalingen
- 20 Hoe gaat SCA alternatieve betaalmethoden beïnvloeden
- 21 Hoe kunnen merchants zich voorbereiden op SCA

Deel 3

23 **Mollie en PSD2**

Afkortingen

2FA

Twee-Factor-Authenticatie

AIS

Account Information Services
Accountinformatiediensten

AISP

Account Information Service Provider
Accountinformatiedienstverlener

API

Application Programming Interface

EC

Europese Commissie

EEA

European Economic Area
Europese Economische Ruimte, EER

EU

European Union
Europese Unie

PIS

Payment Initiation Services
Betaalinitiatiediensten

PISP

Payment Initiation Service Provider
Betaalinitiatiedienstverlener

PSD1

The First Payment Services Directive
De Eerste Richtlijn voor Betaaldiensten

PSD2

The Revised Payment Services Directive
De Herziene Richtlijn voor Betaaldiensten

PSP

Payment Service Provider
Betalingdienstverlener

SCA

Strong Customer Authentication
Sterke Klantauthenticatie

SEPA

Single Euro Payments Area
Eengemaakte Europese Betaalmarkt

TPP

Third-Party Provider
Externe Leverancier

Wat betekent PSD2 voor jouw e-commerce bedrijf

Zoals de meeste e-commerce retailers binnen de EU, vraag je je waarschijnlijk af hoe de nieuwe PSD2-regels van invloed zullen zijn op de manier waarop jij online betalingen ontvangt. Het is een belangrijk aandachtspunt, gezien hoe ontzettend belangrijk het betalingsproces is voor de online klantervaring. Als een retailer wil je dat alles gladjes verloopt, zodat je klant zijn/haar bestelling zonder aarzelen kan plaatsen. Een positieve, professionele betaalervaring geeft vertrouwen en helpt je bij het aantrekken en vasthouden van loyale klanten.

We weten dat er veel vragen zijn omtrent de nieuwe PSD2-regels en dan met name over de vereisten van strong customer authentication (SCA). Hoe gaan deze eisen het betaalproces beïnvloeden? Zal het klanten weggagen wanneer ze extra identificatiestappen moeten doorlopen om een online aankoop te doen? Het is belangrijk om te onthouden dat je niet alleen bent. Alle e-commerce retailers werkzaam binnen de Europese Economische Ruimte (EER) zullen zich aan dezelfde regels moeten houden. En zoals bij iedere verandering van regelgeving, zullen Europese klanten snel gewend zijn aan extra beveiligingsstappen, ondanks dat het wat aanpassingen vergt.

Als retailer kun je het beste maar goed geïnformeerd blijven en er voor zorgen dat je een soepele overgang naar de nieuwe regels kunt bieden. Deze gids geeft een volledige overzicht van alle recente ontwikkelingen, inclusief de huidige tijdslijn voor SCA-implementatie.

Onthoud maar: wanneer je Mollie als payment service provider voor jouw website gebruikt, dan hebben we alles al voor je geregeld. De Mollie API is al aangepast en zorgt voor SCA-compliance voor alle betaalmethoden die we binnen Europa ondersteunen. Toch willen we er voor zorgen dat iedereen de nieuwe regels helemaal begrijpt, zodat je de juiste keuzes kunt maken voor jouw bedrijf en jouw klanten. Dat is waar deze PSD2-gids voor bedoeld is.

Betalingen naar het digitale tijdperk brengen

Digitaal betalen is niet meer weg te denken uit het leven van miljoenen Europeanen. Zorgen voor een veilig online betaalproces voor deze consumenten is een belangrijk aandachtspunt voor merchants en de payment service providers die de betalingen namens hen uitvoeren.

De Revised Payment Services Directive (PSD2) van de Europese Unie zorgt voor een aardverschuiving binnen het betalings- en banklandschap. Het doel is om sneller, handiger en veiliger betalingsverkeer mogelijk te maken, geleverd door een groot aantal verschillende service providers (niet alleen banken).

PSD2 ging op 13 januari 2018 in werking. Een van de belangrijkste bepalingen daarin is 'strong customer authentication' (SCA), wat verplicht gebruik van twee-factor-authenticatie (2FA) betekent voor alle online betalingen binnen de EER.

Na de inwerkingtreding van PSD2 heeft de Europese Bankautoriteit (EBA) **de handhaving van SCA uitgesteld** tot 31 december 2020, om een passende overgangperiode mogelijk te maken. Dit betekent dat payment service providers (PSPs) wettelijk gezien geoorloofd betalingen zonder de twee-factor-authenticatie kunnen blijven uitvoeren totdat SCA daadwerkelijk in werking treedt.

De specifieke deadline voor SCA-handhaving varieert enigszins tussen de Europese landen.

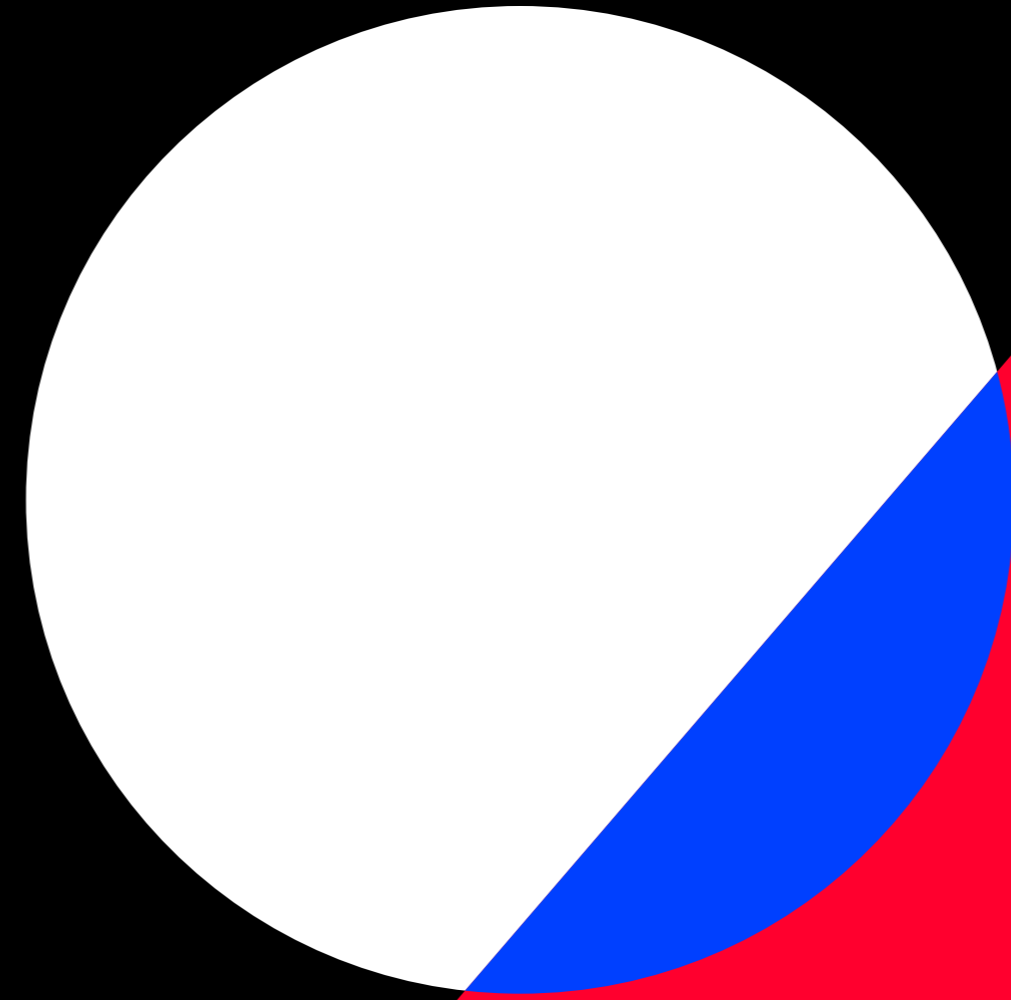
Bijvoorbeeld:

- In de meeste Europese landen, inclusief enorme e-commerce markten zoals Duitsland, Nederland en België, hebben financiële autoriteiten laten weten dat ze de EBA-deadline van 31 december 2020 aan zullen houden.
- Frankrijk heeft eveneens aangekondigd dat het van plan is vast te houden aan de EBA-deadline van 31 december 2020, maar dat het een extra periode van drie maanden kan toestaan in specifieke gevallen.
- Intussen heeft de Financial Conduct Authority in het Verenigd Koninkrijk aangekondigd dat het payment service providers tot 14 September 2021 geeft om SCA in de praktijk te brengen. Dit verlengde uitstel is een direct gevolg van de COVID-19 pandemie.

Door dit uitstel toe te staan, hopen de EBA en nationale autoriteiten de implementatie in goede banen te leiden en payment service providers (PSPs) en banken zo genoeg tijd te geven de nieuwe veiligheidsstandaarden voor online betalingen door te voeren.

Deel 1

Wat is PSD2



“

Als het gaat om online kopen, wil PSD2 online betalen net zo veilig maken als betalen in de winkel.

Kasia Fransen,
Advocaat bij Mollie



De Revised Payment Services Directive (PSD2) is een Europese verordening die tot doel heeft de betaalmarkt open te stellen voor meer concurrentie en tegelijkertijd betalingen veiliger te maken. Het gaat om regels die van toepassing zijn op merchants, banken, consumenten en de e-commerce-industrie als geheel.

Hoewel PSD2 117 artikelen heeft, is een van de belangrijkste veranderingen de introductie van Strong Customer Authentication (SCA) binnen de EER. SCA vereist het gebruik van twee-factor-authenticatie voor online betalingen.

Voor consumenten betekent SCA extra veiligheid. Voor merchants en payment service providers betekent het betere bescherming tegen betalingsfraude en een kans om je klanten beter van dienst te zijn.

Waarom PSD2

PSD2 herzielt de vorige Payment Services Directive (PSD1), die in 2007 opgesteld werd door de Europese Commissie (EC) en in 2009 in werking trad. Het doel van PSD1 was om concurrentie binnen de betalings- en financiële dienstensector in Europa aan te moedigen en tegelijkertijd consumentenbetalingen veiliger te maken.

Dankzij PSD1 werden PSPs onderworpen aan regelgeving en toezicht. De wet bevorderde ook het gebruik van pan-Europese betalingen en concurrentie in de Single Euro Payments Area (SEPA).

Wat concurrentie betreft, hielp PSD1 de betaalmarkt open te stellen voor niet-bancaire bedrijven. Dit heeft geleid tot veiligere en makkelijkere betalingen voor Europese consumenten.

De Single Euro Payments Area (SEPA)

SEPA is een betaalsysteem, opgezet door de Europese Unie (EU), dat alle elektronische betalingen in euro's in de gehele EU samenbrengt. Dankzij SEPA gaat betalen voor een consument over Europese grenzen heen net zo makkelijk en handig als betalen in eigen land. Het stelt Europese consumenten ook in staat om eenvoudig te betalen met hun normale kaart en bankrekening, wanneer ze buiten hun eigen land door Europa reizen.

Van PSD1 naar PSD2

Digitale technologieën en e-commerce zijn drastisch veranderd sinds de inwerkingtreding van de oorspronkelijke PSD1. Deze veranderingen ontstonden eigenlijk deels door PSD1 zelf, wat leidde tot een toename van het aantal financiële technologiebedrijven (fintech) die betaaldiensten aanbieden.

Deze bedrijven hebben de manier waarop betalingen werken veranderd. Ze maken gebruik van technologie om betere betalingsproducten te leveren dan banken. Sommige van deze nieuwe bedrijven en diensten waren echter niet voldoende gereguleerd onder PSD1. De opkomst van snelle, digitale en steeds meer mobiele betalingen heeft nieuwe uitdagingen met zich meegebracht, zoals online fraude, witwassen van geld en financieren van terrorisme.

Zoals elk goed vervolg, gaat PSD2 verder waar PSD1 was gebleven. Dankzij SCA biedt het nu betere bescherming voor de hedendaagse consument bij het doen van online betalingen. Het beschermt ook merchants en payment service providers tegen het risico van frauduleuze betalingen.

Wat is een API?

Application Programming Interfaces (APIs) maken communicatie tussen platforms en apps mogelijk. Voorbeelden van hoe APIs werken binnen PSD2 kunnen bijvoorbeeld zijn: een app van een externe partij waarmee je de saldi van al je bankrekeningen kunt bekijken, of een app waarmee een externe partij namens jou betalingen via jouw rekening kan doen.

“

PSD2 is een consumentvriendelijke richtlijn. Het draait om het beschermen van consumenten en het waarborgen van de veiligheid van hun geld door veel voorheen ongereguleerde diensten onder het toepassingsgebied te brengen.



Sarah Roberto,
Hoofd Compliance
bij Mollie



Wie is wie
binnen
het PSD2
landschap?

Banken

PSD2 draait grotendeels om het beschikbaar stellen van bankgegevens aan andere financiële dienstverleners. Deze externe partijen gebruiken APIs om toegang te krijgen tot deze bankgegevens met toestemming van rekeninghouders. Banken zullen ook worden verplicht om twee-factor-identificatie (SCA) in te zetten wanneer rekeninghouders online een aankoop doen via hun bankrekening.

Merchants

Merchants doen en ontvangen betalingen in ruil voor goederen en diensten. Onder PSD2 zullen ze te maken hebben met al de andere soorten instellingen zoals hierboven beschreven.

Payment initiation service providers (PISPs)

De tweede categorie bedrijven gedefinieerd in de PSD2's XS2A-richtlijnen; dit zijn bedrijven die toegang hebben tot de bankrekening van de consument en namens hen met hun toestemming betalingen kunnen doen. Consumenten kunnen hun toestemming op elk moment intrekken.

Account information service providers (AISPs)

Dit is een van de nieuwe soorten instellingen die door PSD2 zijn aangemaakt in de 'access to account' (XS2A) richtlijnen. Ze kunnen alle bankrekeninggegevens van meerdere bankrekeningen van een consument verzamelen, waarmee ze een centraal overzicht van al hun financiële gegevens bieden. Dit mag alleen met de uitdrukkelijke toestemming van de consument, die op elk moment kan worden ingetrokken.

Payment services providers (PSPs)

PSPs bieden merchants een digitaal platform waarop ze al hun online betalingen kunnen uitvoeren.

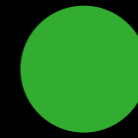
Third-party providers (TPPs)

Dit zijn gereguleerde bedrijven die diensten en producten leveren die verband houden met de bankrekeninggegevens van consumenten. Dit kunnen banken of niet-bancaire instanties zijn. De PSD2 maakt onderscheid tussen twee nieuwe soorten TPPs: account information service providers en payment initiation service providers.

Deel 2

Het effect van PSD2 op merchants

Strong customer authentication (sterke klantauthenticatie)



PSD2 verandert de manier waarop betalingen en e-commerce werken door twee-factor-authenticatie te vereisen voor alle online betalingen. Dit is een wijziging die gevolgen zal hebben voor alle online retailers en hun klanten.

Gelukkig voor winkeliers die Mollie als hun payment service provider gebruiken, hebben wij onze API al bijgewerkt en ervoor gezorgd dat deze volledig voldoet aan de nieuwe regelgeving. Ons doel is ervoor te zorgen dat het afrekenen zo soepel en gemakkelijk blijft gaan als altijd.

Toch weten we dat er veel vragen zijn over SCA en hoe dit de e-commerce in de toekomst gaat beïnvloeden. Daarom geven de onderstaande secties inzichten over SCA en wat het gaat betekenen voor verkopers en klanten.

Twee-factor-authenticatie

Deze vorm van authenticatie vereist dat de consument twee soorten informatie (of 'factoren') verstrekt om een betaling te voltooien.

Consumenten kunnen bijvoorbeeld een betaling verifiëren met hun vingerafdruk (factor één) op hun telefoon (factor twee), in overeenstemming met de SCA-regels van PSD2.

De twee factoren moeten altijd uit twee van de drie hierboven genoemde categorieën afkomstig zijn (iets dat een consument 'heeft, weet of is'). Met andere woorden, betalingen kunnen niet worden geverifieerd met twee factoren uit de categorie 'kennis', zoals een wachtwoord en een pincode.

Als betalingen niet op basis van twee factoren worden geverifieerd, zal de bank de betaling weigeren en gaat de transactie niet door. De uitgevers van een kaart (meestal banken) zijn zelf op de eerste plaats verantwoordelijk voor het naleven van SCA.

Waarom strong customer authentication (SCA)

Betalingsfraude is een groeiend probleem binnen de financiële wereld. In het Verenigd Koninkrijk en Duitsland, de twee grootste e-commercemarkten van Europa, gebeurt **nu meer dan de helft van betalingsfraude** online. Winkeliers, financiële instellingen en consumenten maken zich dan ook grote zorgen over de veiligheid van online betalingen.

Met PSD2 hoopt de EU deze trend te keren. Onder de nieuwe wet is strong customer authentication (SCA) de belangrijkste beveiliging, bedoeld om betalingen veiliger te maken.

Simpelweg betekent dat, wanneer een consument binnen de EER online iets wil kopen, hij/zij tijdens het afrekenen aanvullende authenticatiestappen moet uitvoeren om te verifiëren dat hij/zij daadwerkelijk de kaarthouder is.

Zodra SCA ingaat, moet iedere door de consument geïnitieerde online betaling worden geverifieerd door tenminste twee van de volgende factoren:

iets wat een consument heeft (bijvoorbeeld een telefoon)

iets wat een consument weet (bijvoorbeeld een pincode)

iets wat een consument is (bijvoorbeeld fysiek bewijs dat ze zijn wie ze zeggen, zoals een vingerafdruk of zelfs hun gezicht.

Veel telefoons zijn tegenwoordig al uitgerust met vingerafdruk- en gezichtsscanners).

Hoe hebben merchants voordeel bij SCA

SCA beschermt merchants tegen het risico van de ontvangst van frauduleuze of anderszins illegale online betalingen. Hoewel het een extra stap (twee-factor-authenticatie) betekent in het betalingsproces, staat de wet in veel gevallen ook uitzonderingen op deze stap toe:

Merchant-geïnitieerde betalingen

Bepaalde betalingen die door merchants worden geïnitieerd kunnen worden vrijgesteld. Zo vallen bijvoorbeeld periodieke betalingen in variabele bedragen en betalingen die met onregelmatige tussenpozen worden gedaan op basis van gebruik niet onder SCA.

Transacties van lage waarde

Transacties onder de €30 zijn vrijgesteld van SCA totdat dezelfde kaart vijf keer van deze vrijstelling gebruik heeft gemaakt. SCA is ook vereist vanaf het moment dat de vrijgestelde betalingen in totaal meer dan €100 bedragen. Als een consument bijvoorbeeld drie betalingen van €30 met één kaart doet en vervolgens probeert een vierde betaling van €30 te doen zou SCA vereist zijn, omdat de vierde betaling het totale vrijgestelde bedrag boven de €100 uit laat komen.

Periodieke betalingen

Veel betalingen worden op abonnementsbasis automatisch afgeschreven. De SCA-regels stellen dit soort betalingen vrij zolang ze altijd voor hetzelfde bedrag zijn (bijvoorbeeld een periodieke maandelijkse betaling van €9,99). De eerste betaling in de reeks is echter onderworpen aan SCA, die vervolgens het mandaat verleent voor de betalingen die daarop volgen.

Betrouwbare ontvangers

Onder deze vrijstelling kunnen klanten merchants vooraf goedkeuren of op de 'witte lijst' zetten om te voorkomen dat ze SCA moeten uitvoeren wanneer ze artikelen bij hen kopen. Een consumentenlijst met bedrijven op de witte lijst wordt opgeslagen bij hun bank of PSP.

Betalingen met een laag risico (transactie risico analyse)

Als de merchants payment provider of de bank van de consument fraudepercentages op kaartbetalingen onder de volgende drempels laat zien, kan vrijstelling voor SCA worden gegeven:

- 0,13% om transacties onder de €100 vrij te stellen voor kaartbetalingen op afstand (0,015% voor overschrijvingen)
- 0,06% om transacties onder de €250 vrij te stellen voor kaartbetalingen op afstand (0,01% voor overschrijvingen)
- 0,01% om transacties onder de €500 vrij te stellen voor kaartbetalingen op afstand (0,005% voor overschrijvingen)

Fraudepercentages onder 0,01% betekenen bijvoorbeeld dat transacties van minder dan €500 niet onderhevig zijn aan SCA.

Anonieme kaarten

Anonieme / prepaidkaarten vallen niet onder SCA. Betaalmethoden zoals Paysafecard en cadeaukaarten zijn vrijgesteld van SCA omdat ze anoniem en prepaid zijn, wat betekent dat ze niet onder de SCA-regels vallen.

MOTO-transacties

Mail-order and telephone-order (postorder- en telefonische) transacties zijn vrijgesteld van SCA, omdat SCA alleen betrekking heeft op elektronische / digitale transacties.

Fricctie

Stel je voor dat je klant probeert te betalen voor zijn/haar bestelling, maar wordt gevraagd een eindeloze reeks aan informatie in te voeren. Of dat je webwinkel niet de betaalmethode biedt die de klant verkiest. Dit zijn 'frictiepunten': momenten waardoor consumenten minder gewillig zijn het betalingsproces af te ronden.

Er kan ook 'frictie' in authenticatieprocessen bestaan. Hoe meer informatie je klanten moeten invoeren om een transactie te verifiëren, hoe meer 'frictie' het proces kent. SCA kan voor meer 'frictie' zorgen door twee-factor-authenticatie te vereisen, maar PSD2 probeert een evenwicht te vinden tussen betalingsgemak en veiligheid door uitzonderingen of gevallen waarin authenticatie niet vereist is toe te staan.

Hoe vraag je SCA-vrijstellingen aan

Partijen die SCA-vrijstellingen aanvragen (bijvoorbeeld PSPs zoals Mollie) kunnen slechts één vrijstelling per betalingsverzoek aanvragen. We vragen deze vrijstellingen aan bij de bank van de consument, die uiteindelijk bepaalt of de betaling SCA vereist of niet. We kunnen ook de kaartuitgever (de bank van de consument) helpen beslissen of een vrijstelling moet worden toegepast, door ze bijvoorbeeld aanvullende gegevens te sturen over de consument die een betaling doet, zoals het apparaat waarop ze de betaling doen, het verzendadres dat ze hebben opgegeven of de betalingsgeschiedenis van de betreffende merchant.

Wie is verantwoordelijk voor SCA-compliance

De naleving van SCA is grotendeels de verantwoordelijkheid van de banken die debit- en creditcards aan klanten uitgeven. Hoewel PSPs niet direct verantwoordelijk zijn voor SCA-compliance, moeten we er toch voor zorgen dat onze platforms twee-factor-authenticatie protocollen ondersteunen, zoals 3D Secure en 3D Secure 2.0.

PSPs moeten ook over vrijstelling mechanismen beschikken om die gevallen te behandelen waarvoor twee-factor-authenticatie wellicht niet nodig is. Door over deze hulpmiddelen te beschikken, vergroten PSPs het behoud van betalingen, bevorderen ze een veilige betalingsomgeving en maken ze het (door vrijstellingen toe te staan) makkelijker voor klanten om te betalen.

Wat is het effect van SCA op kaartbetalingen

Onder PSD2 is twee-factor-authenticatie verplicht voor alle creditcard- en debitcardbetalingen die online naar of vanuit een EER-land worden gedaan. Dit betekent dat alle betalingen die worden gedaan met kaarten van bijvoorbeeld het merk Visa, Mastercard of American Express (Amex), onderhevig zijn aan SCA.

3D Secure

3D Secure is een beveiligingsprotocol dat momenteel voor kaartbetalingen wordt gebruikt. Het is overgenomen door de drie grootste kaart maatschappijen in Europa (Visa, Mastercard en Amex). Dit protocol vereist dat consumenten extra informatie invoeren om hun identiteit te verifiëren bij het doen van een aankoop. Het is ook SCA-compliant. Veel kaartgebruikers in heel Europa maken al gebruik van 3D Secure bij het doen van online aankopen.

Hoewel 3D Secure SCA-compliant is, komt er binnenkort een nieuwe versie: 3D Secure 2.0. Deze versie wordt de primaire optie voor SCA-compliance onder PSD2.

Nieuw onder 3D Secure 2.0 is dat kaartgebruikers wanneer authenticatie nodig is nu 'frictieloze authenticatie' kunnen doorlopen, met behulp van biometrische gegevens of een wachtwoord. De toevoeging van biometrische gegevens, zoals vingerafdrukken, maakt de betalingservaring voor consumenten eenvoudiger en veiliger.

'Frictieloze authenticatie' wordt gebruikt bij uitzonderingen. Wanneer een consument een kaartbetaling wil doen die voor een vrijstelling in aanmerking komt, kan deze worden goedgekeurd zonder verdere input van de consument. Dit vereenvoudigt het betalingsproces, waardoor het verlaten van de winkelwagen tijdens het afrekenen wordt voorkomen.

Hoe gaat SCA alternatieve betaalmethoden beïnvloeden

Onder niet-creditcardbetaalmethoden (ook bekend als 'alternatieve betaalmethoden') vallen opties zoals Apple Pay, PayPal, Klarna, bankoverschrijvingen en cadeaukaarten.

In Europa vereisen veel van deze methoden al twee-factor-authenticatie. Apple Pay-betalingen moeten bijvoorbeeld worden geverifieerd via het apparaat van de gebruiker, met zijn/haar gezicht of vingerafdruk. Ondertussen vereisen bankoverschrijvingen vaak authenticatie met behulp van een apart apparaat waarin een gebruiker een toegangscode invoert.

Cadeaukaarten die anoniem en prepaid zijn vallen buiten de SCA-regels. Dit betekent dat ze geen twee-factor-authenticatie vereisen.

Hoe kunnen merchants zich voorbereiden op SCA

De SCA-regels onder PSD2 zijn belangrijke nieuwe regels die elke online retailer in de EU moet kennen. Hier volgt een aantal zaken dat je kunt doen om je voor te bereiden op naleving van deze nieuwe regels:

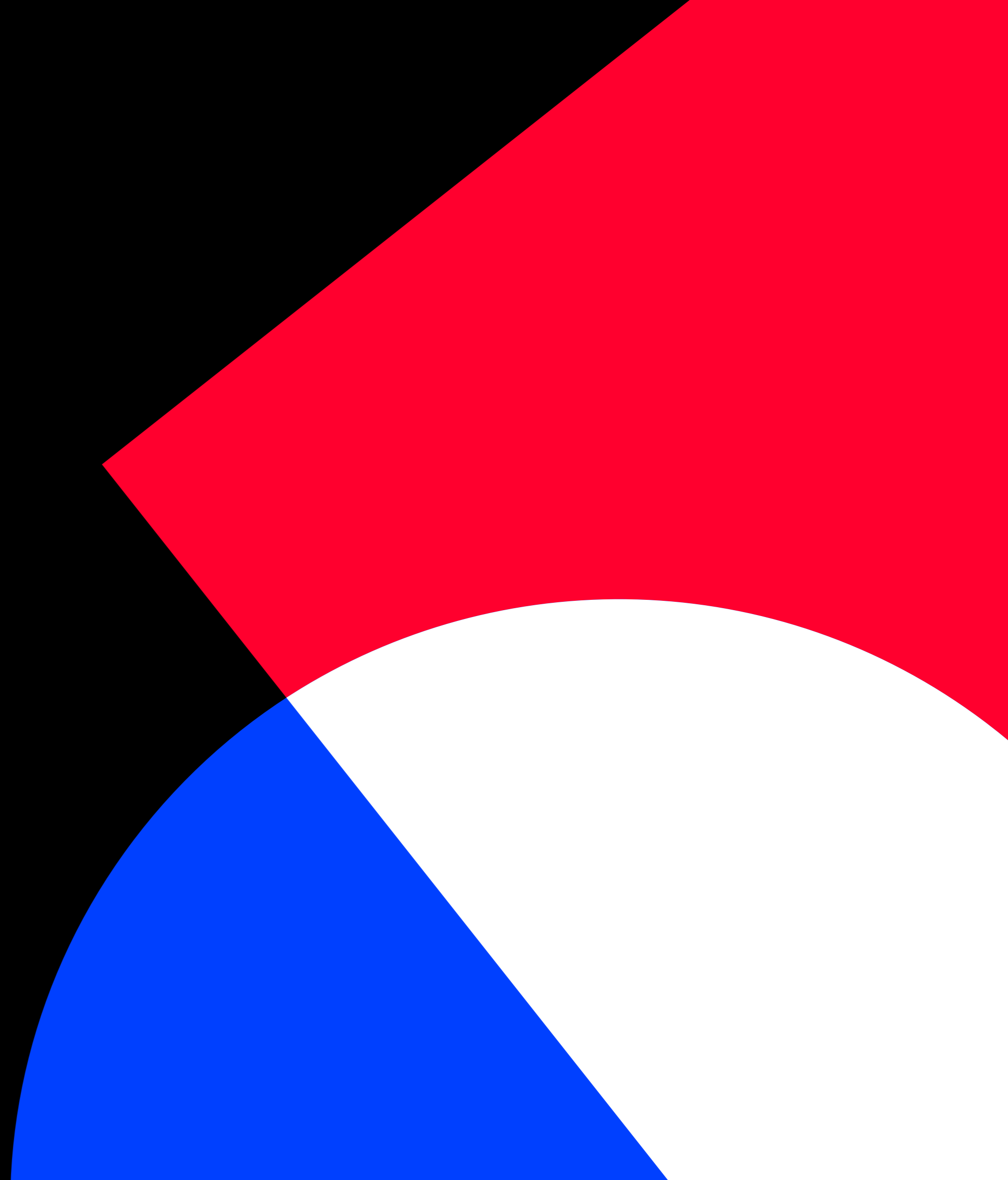
- Informeer je klanten over op handen zijnde veranderingen
- Begrijp wat je zakelijk gezien nodig hebt met betrekking tot SCA

Communiceer open en transparant met je klanten over de nieuwe SCA-regels. Informeer hen ruim van tevoren dat er mogelijk extra stappen in je afrekenproces komen zodra de regels in werking gaan. Maak vooral duidelijk dat deze stappen het afrekenproces veiliger maken. Als je klanten weten wat ze kunnen verwachten, zijn ze zelf beter voorbereid en zullen ze minder snel hun winkelwagen verlaten bij extra betaalstappen.

Om aan de behoeften van je onderneming te voldoen is het belangrijk dat je een payment services provider hebt die SCA ondersteunt, inclusief vrijstellingen. Werk samen met een PSP die over de juiste tools beschikt om je te helpen voldoen aan SCA en tegelijkertijd de best mogelijke klantervaring te bieden. Onthoud dat het doel van SCA is om een veilige betalingsomgeving te creëren en het risico van geweigerde betalingen als gevolg van niet naleven te verminderen. Hoewel het even wennen is, zal het je uiteindelijk helpen om klanten te behouden door hun vertrouwen te winnen.

Deel 3

Mollie en PSD2



Sinds de invoering van PSD2 heeft Mollie ervoor gezorgd dat ons platform volledig voldoet aan de nieuwe SCA-vereisten die op 31 december 2020 in de meeste Europese landen in werking gaan. Onze API is up-to-date en voldoet aan SCA-compliance. Mollie-gebruikers hoeven zelf niets te doen. We zijn er helemaal klaar voor.

Met Mollie kun je je klanten via ons platform veel verschillende betaalmethoden aanbieden. Of het nu gaat om iDEAL, SEPA-overschrijvingen, Apple Pay, kaartbetalingen of andere. De meeste van deze betaalmethoden zijn al SCA-compliant, omdat ze twee-factor-authenticatie vereisen voordat de klant een betaling kan afronden. Met Apple Pay verifieert een klant bijvoorbeeld zijn/haar identiteit met behulp van zijn/haar telefoon (iets wat hij/zij heeft) en vingerafdruk of gezicht (iets wat hij/zij is).

Intussen ondersteunen we ook het SCA-compliant 3D Secure-protocol voor Visa, Mastercard / Maestro en American Express-kaarten. En we supporten 3D Secure 2.0 volledig, inclusief vrijstellingen, zodra iedere uitgever van creditcards overschakelt op het gebruik van dit protocol.

“

Veel merchants vragen zich af: ‘Moet ik PSD2-compliant zijn’? Je moet compliant zijn wanneer je diensten aanbiedt die onder PSD2 vallen. Voor de overgrote meerderheid van merchants is dit niet het geval, omdat betalingen worden verwerkt via een PSP die compliant is, zoals Mollie.

Sarah Roberto,
Hoofd Compliance bij Mollie



SCA-compliant betaalmethoden ondersteund door Mollie



**Wil je meer weten
over hoe je de
aankoopervaring voor
je klanten makkelijker
kunt maken?**