entersekt

and you're in.

Beyond compliance:

A 3D Secure ACS and payment authentication solution for today's digital economy

Table of contents

Foreword

A data-open approach for a brighter banking future

It's clear that the pandemic fast-forwarded online consumer behavior, while merchants kept step pace with their consumers and innovated to meet them where they are — in their home office or living room armchair. In fact, the **number of consumers** performing more than half of their shopping online increased from 31% to 57% from pre- to post-pandemic.

But, as is often the case, with new trends come new opportunities for fraudsters to exploit the system. And, in 2021, card-not-present (CNP) fraud constituted **85% of all card fraud**.

We find that CNP fraud is dominated by cyberattacks, such as social engineering fraud, sometimes in collaboration with account takeover attacks, and chargeback and friendly fraud. Unfortunately, these types of fraud are becoming increasingly difficult to detect and protect the cardholder against.

However, by utilizing a modern approach — with acceptable friction — financial institutions can deliver a secure in-purchase-flow authentication experience built on the 3D Secure protocol.

Our cloud or yours?

Entersekt focuses on providing an EMV 2.2 certified access control server (ACS) that enables modern cardholder authentication experiences through built-in end-to-end OTP, app-free and in-app authentication journeys.

Our ACS provides issuers with full control of the user experience through self-service configuration options. Plus, the flexibility to choose between client-hosted or SaaS deployment options depending on their unique requirements. Our only question: our cloud or yours?

With simple, configurable self-service cardholder authentication journeys, utilizing modern authentication technologies and real-time API integration, issuers can personalize each cardholder transaction. The result — improving authentication success rates by 54% and achieving market leading approval rates in excess of 90%.

At Entersekt, we offer financial service providers (FSPs) a data-open approach, providing them with access to a rich set of data on consumer behavior, merchant and transactional attributes, risk attributes, and the authentication outcome of transactions. We extend the value of our offering beyond a good payment authentication experience for cardholders, fraud prevention, and cost savings, to supporting business development, and ultimately helping our customers leverage data to drive more successful e-commerce experiences.

Jonathan van der Merwe,
Group Product Manager: Payments

The evolution of 3D Secure and the compliance ecosystem

The world of e-commerce and online transactions is nothing like it was a decade ago. Consider how the pandemic turned the global status quo on its head — permanently changing how consumers around the world purchase goods and services. In 2021, global e-commerce sales totaled approximately $5.2 trillion. By 2026, online retail figures are forecast to reach over $8 trillion worldwide. People learned to adapt and be resilient – with the help of technology.

But it was not only human habits that needed to change fast. With the rapid adoption of mobile as an essential purchase channel, for instance, the mechanisms that keep customers' transactions safe also had to evolve at pace.

This more expansive CNP payment landscape opened up many opportunities for merchants and FSPs to differentiate and grow their bottom line. But it also opened the playing field to new fraud vectors. CNP fraud is predicted to reach over $49 billion globally by 2030.

Fortunately, regulatory compliance, such as 3D Secure and the Payment Services Directive (PSD), is constantly updated to protect and secure customers' data, however they choose to transact online. In Europe, regulations such as PSD2 and Strong Customer Authentication (SCA), are laying the foundation for FSPs to ensure safe, seamless customer payments across a broad range of channels. However, in the United States, the regulatory landscape has some catching-up to do in order to fall in line with global best practice. The technology in this changing digital environment needs to balance the security of online transactions with a seamless customer experience — one that doesn't leave consumers feeling frustrated. In fact, reaching this balance is key to reducing payment fraud and chargebacks, and increasing conversions and revenue. A recent PYMNTS and Entersekt survey revealed that 80% of consumers want a good user experience, with 60% of respondents stating that security was critical too.

From large issuers to credit unions, FSPs rely on a dynamic, supportive compliance ecosystem of standards and technology that can adapt quickly and keep fraudsters at bay.

Advances in authentication standards

Maintaining a payment experience that is safe and hassle-free in an ever-changing global threat landscape means that the guiding standards and regulations must adapt continually to support merchants and FSPs.

Vital advances, like the shift from 3D Secure version 1 to EMV 3-D Secure, help to keep the compliance ecosystem protocols on par, and able to supply the context needed for secure, real-time authentication.

Let's examine the development of these core industry standards.

3D Secure

The first version of 3-domain server, or 3D Secure, was developed by Visa in 1999 as a technical standard to protect consumers and merchants from payment fraud. The standard delivered an added layer of security for all online payments. Typical implementations often defaulted to username and password combinations, while in some parts of the globe, FSPs used SMS OTPs. However, the constraints of bad design and outdated authentication technology had such a negative impact on the customer experience, adoption was never widespread.

Recently, after two decades of an ineffective version 1, version 2 (or EMV 3-D Secure) was introduced, offering a less intrusive checkout experience and a fresh start for FSPs and merchants. The upgraded protocol now supports the channels that today's consumers use to transact – with app-based authentication to support mobile devices, and EMV 3-D Secure only challenging transactions assessed as higher risk (or as mandated under PSD2).

Payment Services Directive

The Payment Services Directive (PSD) is an electronic payment regulation for Europe, first introduced in 2007 to reduce fraud. The Second Payment Services Directive (PSD2) was introduced in 2016. While it also aims to reduce fraud, the revised version focuses more on supporting retail payment innovation and competition.

PSD2 also improves the payment experience through the use of two-factor authentication, and includes mandates like SCA, and the standard industry protocol, 3D Secure.

In May 2022, the European Commission (EC) published a call for consultation on updating the directive. Like PSD2, PSD3 will focus on SCA and open banking standards and protocols with the aim of streamlining consumers' interactions with both banks and merchants.

The draft version is expected by mid-2023 and will take approximately five years to come into full effect. At Entersekt, we are fully committed to navigating this change when the time comes to enable full compliance within the required timeframe.

Strong Customer Authentication

Strong Customer Authentication (or SCA) was a directive introduced by PSD2 in 2021, requiring digital payment transactions to include multi-factor authentication in the United Kingdom and Europe. The purpose of SCA is to improve the security of online payments by requiring two forms of identification from the customer when they shop online, such as a PIN, the device used, or a biometric confirmation. With this added layer of security, FSPs and customers gained a more modern, reliable method of identity verification, and the resultant reduction in fraud.

Fast IDentity Online

Fast IDentity Online (or FIDO) is a technical specification for digital identity authentication. The FIDO standards, protocols, and specifications were developed by the FIDO Alliance. This open industry body aims to develop better digital and web security that focuses on user authentication, identity verification and binding, and the Internet of Things (IoT).

The original goal of FIDO was to simplify verification while improving digital security. The initial version was closely followed by the upgrade, FIDO2, which aimed to eliminate password use altogether on digital channels. Along with the drive towards passwordless security, FIDO2 also eliminated the traditional threats that accompany username and password logins.

> With 47% of cyberattacks in 2021 reported as sophisticated, it's clear that password authentication alone is not enough.

Today, FIDO2 is one of the benchmarks for current customer authentication. FIDO is continually enabling innovative ways to authenticate online payments with WebAuthn (the official web standard for passwordless logins), such as Secure Payment Confirmation (SPC), helping to balance security and the user experience.

Moving on from outdated passwords and OTPs

Passwords and SMS OTPs are on the way out and opening doors for more modern solutions like biometrics and in-app authentication. Authentication solutions that gather and share contextual data about a user's behavior and identify high-risk interactions in real-time are the way forward for seamless, secure user experiences.

Starting at the earliest and most basic, username and password logins are the most common form of authentication. They're also the easiest for hackers to crack, especially when users reuse passwords across multiple accounts or use simple, one-word passwords like the name of their child or dog. Unfortunately, this outdated and overly simple method creates opportunities for phishing and brute-force attacks.

Taking a step towards improved security measures, we have multi-factor authentication, or MFA. MFA requires two or more additional factors or categories, beyond using only a password. These categories include the knowledge factor or something you know, such as a password or one time password (OTP); the possession factor or something you have, such as your device or SIM card; and the inherence factor or something you are, such as biometrics.

Multi-factor authentication that includes out-of-band authentication, such as an SMS OTP, (when the second factor is from a different channel) slightly elevates the level of security, but the transaction is still vulnerable to man-in-the-middle attacks.

Risk-based authentication, or RBA, passively authenticates a customer by determining behavioral patterns. With RBA, you can silently track a user's behavior, identify high-risk interactions, and continually build up contextual information on their normal user behavior. Any behavior that strays from 'normal' is flagged and triggers further investigation to establish whether the user is who they say they are.

Say for instance a customer is buying their regular weekly groceries online from their home, like they always do on a Saturday morning. Nothing out of the ordinary. So, the transaction is assessed as low risk and the customer's payment goes through without any visible checks. However, if that alleged customer tries to buy three top-of-the-range laptops from another continent on a Tuesday at 23:00, that's highly suspicious. That transaction will be flagged as high

risk and will either be outright declined, or step-up authentication will be implemented to verify that the person making the purchase is who they claim to be.

RBA tracks, identifies, and handles interactions in real-time — silently if the risk is low or with step-up authentication if the risk is high. But in both cases, the user experience is kept both seamless and secure.

What's more, banks using an all-in-one authentication platform (rather than single-channel authentication) derive even more benefit from RBA, enabling intelligent decisions across all their digital channels.

For effective customer authentication that removes all unnecessary friction, leading banks are choosing solutions that offer advanced, cross-channel user journeys. Cross-channel (or omnichannel) authentication breaks down the data silos between channels, improving security and ensuring a seamless and familiar experience for customers.

Looking to the future: Context Aware™ Authentication is key

The future of authentication technology lies in gaining a complete, context-rich picture of both the user and the interaction in real-time and establishing a curated authentication journey for the customer for that specific interaction. We call it Context Aware™ Authentication.

Financial institutions that wish to stay ahead of the game need to think beyond compliance, to create a seamless user journey across all banking channels.

"With online banking and digital payments becoming mainstream, financial institutions cannot afford the fraud risk and negative customer impact of disparate authentication tools. Having a single platform that protects digital, payment, and data channels provides a better user experience while increasing transaction success." *– Frank Moreno, Entersekt Chief Marketing Officer*

Myth versus reality: Four common compliance misconceptions

Achieving and maintaining compliance is mandatory for all FSPs. And though institutions may feel burdened by these complex security standards, such as 3D Secure and PSD2, it is possible to turn compliance into a competitive advantage.

Let's explore and debunk four common myths about compliance that you can use to your benefit.

Myth 1: Your customers will suffer with poor user experience

In the past, 3D Secure 1 was renowned for poor user experience. The authentication protocol had limited operability and slowed down, or even completely prevented, customers from completing a purchase.

The use of single-channel authentication solutions can also result in a poor user experience. Financial institutions that use various solutions for their digital channels create a disjointed authentication experience that is less effective against fraud.

The reality

Context Aware™ Authentication enables Entersekt to offer highly configurable e-commerce authentication journeys that allow banks to configure personalized authentication experiences with speed and across all digital channels. Customers can choose between a broad range of pre-built, configurable user journeys and trigger step-up authentication when needed that remains seamless for the customer.

Myth 2: You'll have no control over your ACS

Some believe that an ACS has limited functionality, allowing little to no control over the customer authentication process or ability to customize various aspects of the customer journey. Preset configurations and no personalization stifle the ability to create a differentiated, seamless customer experience. Yes, that can be the case with many ACS providers. But not all!

The reality

With Entersekt's ACS, you get the configurability that allows you to take control of the solution, enabling rapid iterative changes and delivering the service according to your systems and procedures.

Myth 3: With no control, there's no data

Many ACS providers don't give banks and other FIs access to the data needed to properly verify their customers' identities. Unfortunately, with little to no control of ACS configurability, it stops the flow of data — preventing vital information about who's transacting, when, where, and on what device.

The reality

With Entersekt's ACS, banks are in control of all their data, helping them better understand user and transaction data and make valuable, data-driven decisions in real-time.

Myth 4: Maintaining compliance is a hassle

Issuers may feel like compliance standards and regulations change every day. Yet regular updates help technology keep up with how customers (and fraudsters) interact online.

For FIs that use different standalone compliance and authentication solutions across different channels, it can be arduous to keep all compliance parameters up to date. Many businesses feel that time spent managing and maintaining compliance software could be better spent maintaining their core business. And we agree.

The reality

With Entersekt, you get a solution that maintains compliancy for you so that you don't have to think about it. Our ACS is always 100% up to date with all the latest compliance regulations and standards, freeing up time to focus on operations and driving revenue.

Upping the ante: From 3D Secure 1 to EMV 3-D Secure

In October 2022, 3D Secure version 1 was sunsetted for good. The original authentication protocol was developed more than two decades ago to primarily serve card networks, and operated using SMS OTPs for security. But, with its limited operability, the user experience was often frustrating and led to high cart abandonment rates.

As a result, many merchants found a way to game the system, doing their own risk decisioning and only channeling the highest risk transactions across.

However, since then, the 3D Secure protocol has improved drastically.

A modern take on payment security

To modernize payment security, 3D Secure 2 (or EMV 3-D Secure) was introduced with more data points, choices, security, and use cases. The new protocol now worked with debit networks and other applications, and was broader than card scheme applications alone.

EMV 3-D Secure 2.1 was introduced in 2017 and included mobile payments, enabling native mobile experiences for native merchant app experiences. This newer version of the standard kicked off the ability to drive more accurate risk analysis as it permitted more data to be collected.

The next iteration, version 2.2, introduced risk-based authentication, gathering a broader set of data about the cardholder and transaction, and sending that information to the issuers. Basically, it brought together the issuer, acquirer, and card scheme — further evolving the efficacy of online payments.

The additional data enabled banks to make informed decisions about the level of risk for the transaction, facilitating seamless checkouts. It also allowed issuers to personalize the customer experience and make the authentication process more customer-centric.

Powering up in-app, biometric, and decoupled authentication

3D Secure 2 uses modern authentication solutions, including in-app approval, biometrics, and decoupled authentication to facilitate a seamless user experience.

Decoupled authentication occurs when a transaction happens without the customer necessarily being online. In fact, the customer may not be present at all. Let's say, for example, that you subscribe to Netflix with a recurring payment on your credit card. You input your details and the subscription begins.

In the background, your bank sends you an email with a link asking you to confirm that you have subscribed to Netflix. You don't have to authenticate that payment immediately, but should within the number of days they stipulate.

Basically, the evolution to EMV 3-D Secure means more data, more security and better support for recurring payments and online subscriptions – as well as for travel industry type transactions usually consisting of multiple payments linked to a single authentication.

> The bottom line: 3D Secure 2 enables FSPs to make advanced customizations and access data intelligence to maintain a secure, uninterrupted customer experience. At Entersekt, we support that 100%.

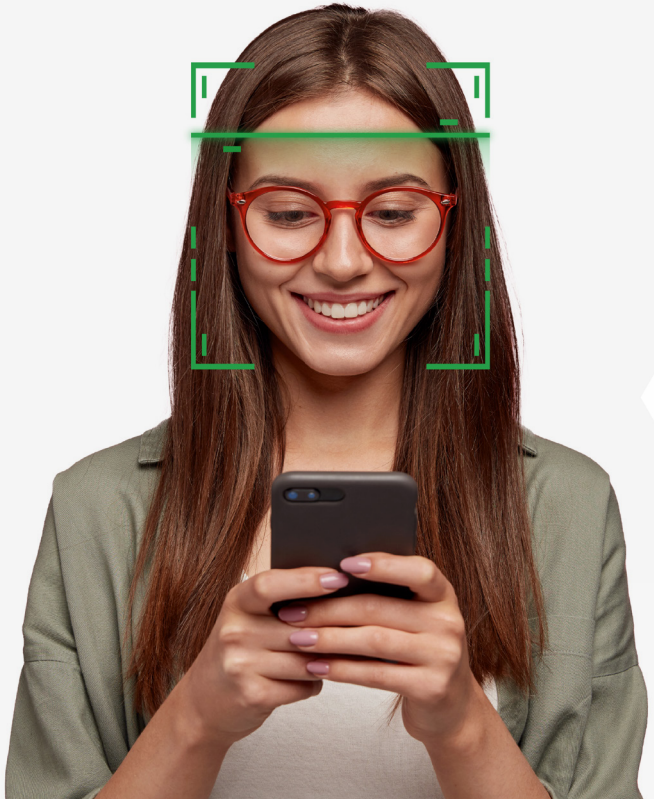
Beyond compliance: Entersekt's 3D Secure ACS

Entersekt is a global leader in customer and transaction authentication, working with card issuers and financial institutions to enable payment authentication that removes unnecessary friction. We provide payment authentication solutions that go beyond compliance, providing world-class e-commerce fraud prevention consistently across all banking channels.

Entersekt delivers a 22% higher transaction success rate than the European average! And our 100% compliant ACS is fully customizable, enabling full control of the user journey down to individual card level, driving higher conversions.

In today's digital payment landscape, banks want a seamless user experience across all channels to ensure vital customer information is shared, continually building a stronger picture of customer identity and reducing fraud. Entersekt provides a context-aware authentication ecosystem that enables organizations to link all components of their business.

"FIs that solely focus on compliance are often subjected to increased end-user friction, high contact center costs, and lost transaction fees resulting from false declines. A balance of continuous compliance with Context Aware™ Authentication will mitigate fraud and regulatory risks while increasing successful transactions and reducing costs." *– Frank Moreno, Entersekt Chief Marketing Officer*



Let’s explore these features in more detail.

ACS feature spotlight

Banking-grade security that reduces fraud and keeps customers safe

Entersekt offers banking-grade security for its customers, enabling payment authentication without adding unnecessary friction. There’s also more control, customization freedom, and access to data that allows you to put your customers first.

Our payment authentication solutions not only have a broader application, including logins, but also provide FSPs with more context on customer transactions. The result is that banks can plug any digital payment security gaps, reduce fraud, and keep customer data safe.

More control and configurability freedom

With Entersekt, banks can customize their ACS solution easily to suit how their business works. Anyone can work with the interface regardless of their technical aptitude. And they can design all their authentication experiences into a practical ecosystem based on business objectives rather than potential technical limitations.

We have two core deployment options: client-deployed (on-premise, client-hosted) or Cloud (SaaS) ACS:

- With Entersekt’s client-deployed ACS, you get full control over the processes that govern your ACS’s operational procedures. By its nature, this option suits medium-to-large issuers that have specific data residency or data processing requirements that necessitate an ACS to be deployed within their own environments.

- Some FIs, like credit unions, prefer to stay focused on their core function and members and leave the technical side of authentication to the experts. Our simple, managed Cloud ACS will keep your business compliant and your customers’ digital transactions safe, without the operational hassle.

Faster deployment

For many issuers, their ACS does not offer the configurability for swift setup and integration. That's not the case with Entersekt.

The Entersekt team is able to set up our all-in-one platform in a matter of days, complete with mock testing tools, such as a merchant website. Customers can then install the ACS and perform end-to-end testing within the space of two hours. With this ease of integration and testing, these FIs also have the space to test and learn our system without the pressure that usually accompanies ACS integrations.

Once our client-deployed ACS is set up, Entersekt's stable, simple interface is easy to implement and integrate for smooth onboarding, and even bulk-onboarding.

Sustained operability with continual innovation

Entersekt is committed to developing cutting-edge fintech solutions that solve real-world industry problems. We hold over 30 technology patents across the globe, from key international patents, such as Interactive Transaction Authentication, ECERT, and Multi-app, Multi-Factor Authentication, to a patent for MNO technology in South Africa that resolved a major gap between SMS OTPs and app-based authentication.

Ultimately, this means our customers have access to the latest technology, built by industry innovators, to continually meet the changing needs of their business and the broader ecosystem.

Entersekt developed the world's first payment use case incorporating 3D Secure and FIDO for the leading German card issuer, PLUSCARD, together with Netcetera.

"Customers without a mobile device now have the option to approve their online payments conveniently and securely with the FIDO token. Together with Netcetera and Entersekt, we have implemented a future-proof solution with the FIDO standard. So far, this is a unique alternative to app-based authentication in the German market."

— Thomas Niederauer, Product Manager, PLUSCARD (2021)

Across the globe: We've got you covered

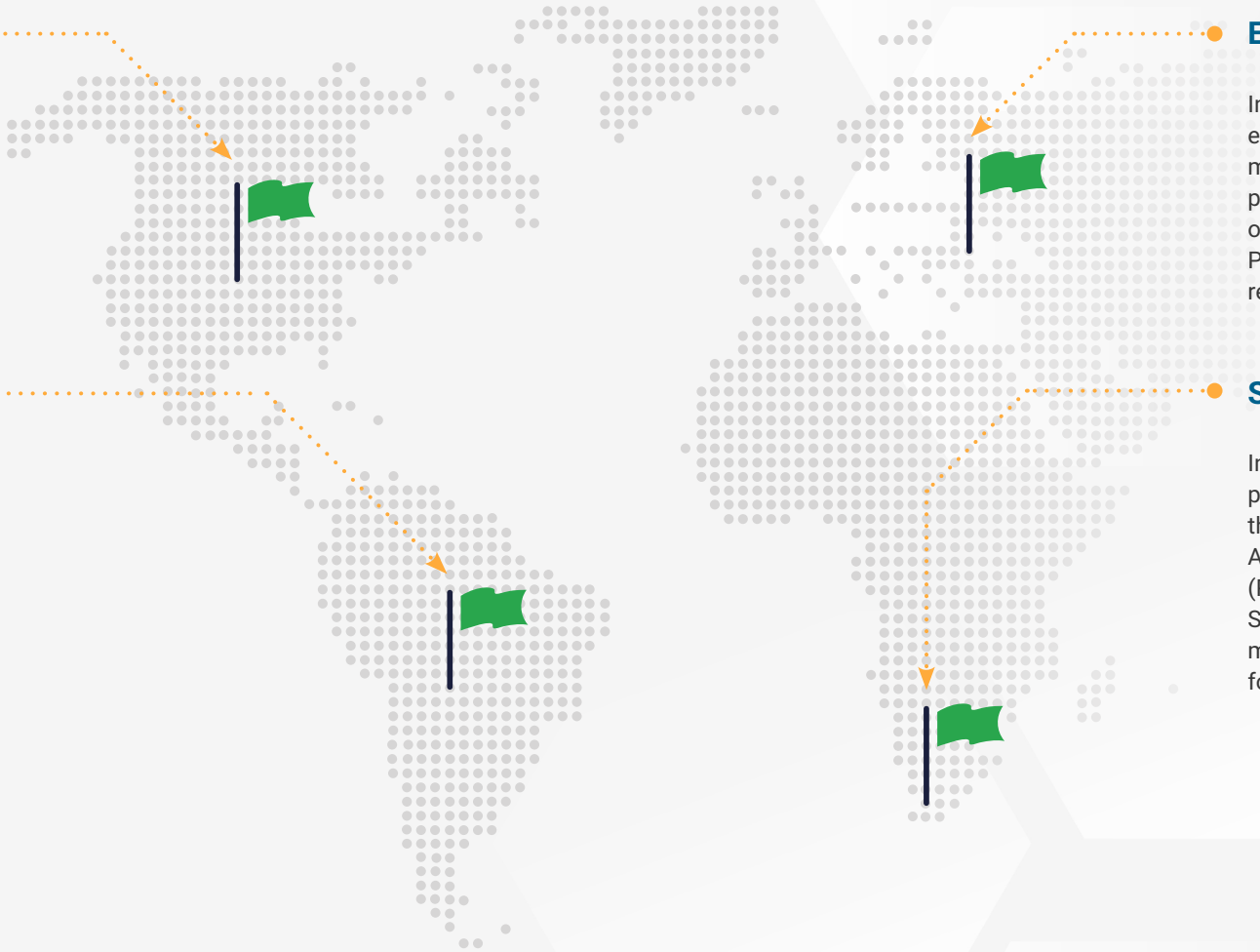
Entersekt offers up-to-date compliance solutions aligned with global payment regulations. Whether it's for PSD2, SCA or 3D Secure, Entersekt provides world-class e-commerce fraud prevention solutions. Across the globe, we've got you covered!

North America

North America holds the largest e-commerce market share. With all major card networks operating in the US, such as Mastercard, Visa and American Express, the adoption and integration of 3D Secure has been growing.

South America

Digital payments in South America are slowly but surely on the rise, even though up until 2020, 45% of Latin Americans did not have a bank account and approximately 80% did not have a credit card.



Europe

In Europe, banking customers enjoy the convenience of mobile banking, but also prioritize payment security over frictionless transactions. Payment regulations for the region include PSD2 and SCA.

South Africa

In South Africa, online payments are regulated through the Payment Association of South Africa (PASA). PASA mandated South African e-commerce merchants to use 3D Secure for all payments from 2014.

Across the globe: We've got you covered

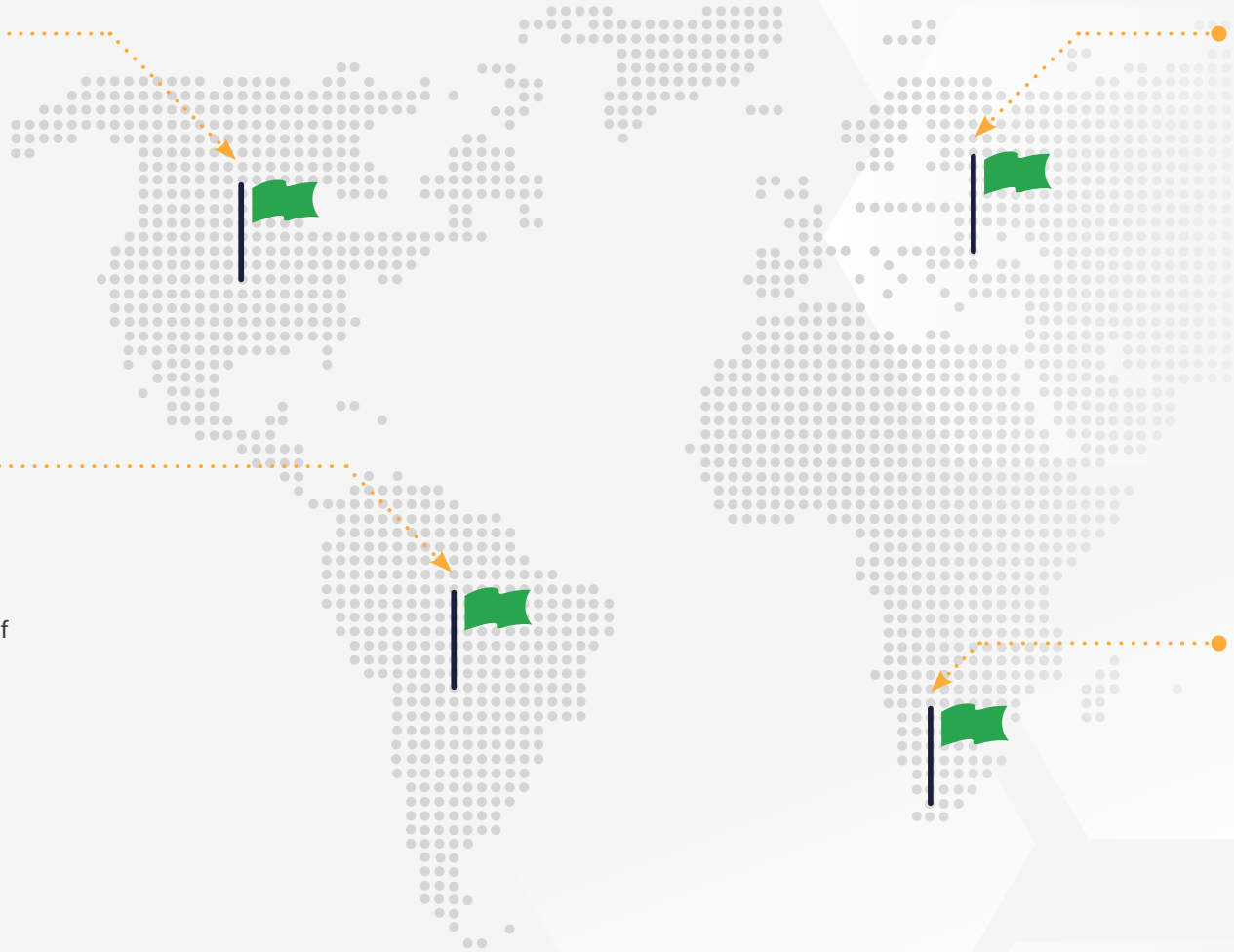
Entersekt offers up-to-date compliance solutions aligned with global payment regulations. Whether it's for PSD2, SCA or 3D Secure, Entersekt provides world-class e-commerce fraud prevention solutions. Across the globe, we've got you covered!

North America

- **Regulations: 3D Secure**
- **3DS share of global market:**
  - The US has 28.9% of the 3Ds global market
- **Top online payment methods:**
  1. PayPal 24%
  2. Visa 13%
  3. Amazon Pay 11%
  4. Apple Pay 10%

South America

- **Regulations: 3D Secure**
- **3DS share of global market:**
  - South America has 3.06% of the global market
- **Top online payment methods:**
  1. 55% Bank transfers
  2. 33% Credit cards
  3. 32% eWallet
  4. 28% Debit cards
  5. 12% other



Europe

- **3DS success rates:**
  - In the UK, 3D Secure uptake is high and improving overall payment security.
  - In countries such as Sweden, Finland, Norway and Demark, 3DS acceptance is between 83-86%.
- **Top online payment methods:**
  1. PayPal
  2. Debit card
  3. Credit card
  4. Klarna
  5. Cash on delivery

South Africa

- **3DS usage:**
  - 99% of e-commerce transactions in South Africa use 3D Secure
- **Top online payment methods:** [15]
  1. 41% Credit card
  2. 20% Bank transfer
  3. 17% eWallet

Customer case study

Capitec Bank boosts payment security: from 3D Secure to real-time authentication

After the Payments Association of South Africa (PASA) mandated the use of 3D Secure, Capitec, South Africa's largest digital bank, took the necessary steps to comply. However, the limitations of 3D Secure version 1 led to low adoption rates. The experience was far from user-friendly, causing cart abandonment rates to soar and frustration among customers.

When the bank reached out to Entersekt, they could begin transforming the payment experience for their customers. From the installation of the Entersekt Secure Platform (ESP), Entersekt has helped Capitec continually update their card-not-present (CNP) payment authentication, reducing fraud and boosting conversion rates.

In 2018, with the implementation of Entersekt's 3D Secure solution, the bank's cardholders no longer needed to rely on passwords, and authentication became an easy, one-tap process — seamless step-up authentication that looked and felt the same as all their online banking transactions.

The next innovation was the addition of pop-up messaging to warn cardholders when they were about to exceed their limit — reducing limit-related declines.

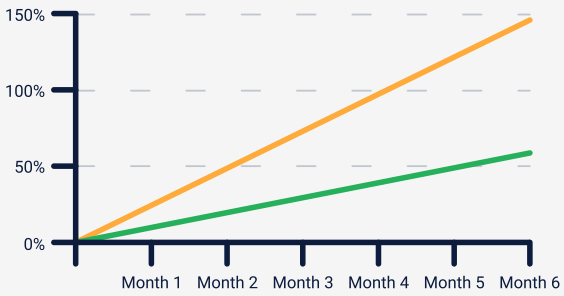
And most recently, in 2022, Entersekt upgraded the bank's payment authentication from 3D Secure 1 to EMV 3-D Secure, further boosting the security of their online payments while reducing friction for their cardholders. The solution incorporates behavioral analytics from NuData Security, a Mastercard company, and enables Capitec to create differentiated e-commerce experiences for their customers.

During checkout, the solution calculates a risk score for each cardholder's transaction. Based on the risk score, a frictionless authentication experience is possible when there's little to no risk. Or in high-risk cases, a step-up authentication process is triggered.

As a result, Capitec can now identify high-risk e-commerce interactions in real-time, significantly boosting security without impacting the customer experience.

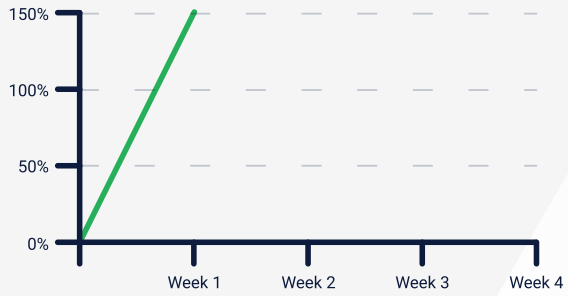
> Learn more about Capitec's upgrade to EMV 3-D Secure with Entersekt **here**.

Capitec case study: Results



Phase 1 [Initial set up]

In six months, transaction success rates increased by **54%**. Transaction value also grew by **149%**.



Phase 2 [After limit pop-up message implementation]

Declines linked to transaction limits fell drastically. And in just over one week, conversion rates increased by **150%**.

> ***"We are constantly looking for ways to offer the best security possible without impacting our customers' experiences. By implementing Entersekt's EMV 3D Secure solution with behavioral analytics from NuData Security, we are able to provide an additional level of protection for our e-commerce transactions. This also allows our team to continue to innovate, keeping our customers secure and Capitec at the forefront of digital banking innovation in South Africa."***
>
> *– Francois Viviers, Executive: Marketing and Communications at Capitec Bank.*

About **Entersekt.**

Entersekt provides transaction authentication to financial institutions that is both secure and free from unnecessary friction. Our single, cross-channel platform empowers these institutions to build great user experiences for their customers, helping to drive revenue growth without adding further costs and complexities to their ecosystems.

For over a decade, we have enabled some of the world's most prominent financial brands with the tools and confidence to conquer fraud, compliance, disparate customer journeys, and the related bottom-line impact of reputational damage and customer loss. Backed by companies like US-based Accel-KKR, one of the world's top private equity firms, Entersekt continues to innovate and expand its global footprint.

For more information about Entersekt, or to speak to an expert, please visit www.entersekt.com or email info@entersekt.com.

/Entersekt

@Entersekt

/Entersekt