3D Secure 2 Takeover:

Top Online Payments Security Trends and Predictions till 2026

asee
by asseco

Summary

1. Introduction

TriDES2

We are witnessing a never before seen increase in yearly eCommerce and digital transactions growth. Although online payments have been around for quite a while, forecasts for the upcoming five years are predicting unmatched figures. Innovation in the online payments sector and accelerated customer adoption of such payment methods are greatly induced by the ongoing Covid-19 pandemic. It is no wonder that online payments are increasing their audience at soaring rates, convenience and accessibility being the key factors for such a shift.

However, among all the benefits provided by online payments, there are always many bad actors looking to overturn the situation to their advantage. That is why security has become imperative. Protecting businesses and cardholders is an ongoing effort when talking about the online payments ecosystem. Regulatory bodies enforce policies involving multi-factor authentication (MFA), data protection, and overall risk assessment procedures. These requirements make security one of the top strategic points for financial institutions, instead of just being a compliance-related matter.

For the past few years, 3D Secure protocol has proven to be an effective solution in preventing malicious attacks in online payments. The new version of the solution, **3D Secure 2**, comes with additional features focusing not only on providing an additional layer of security but offering multiple convenient features. Mentioned features include the ability to select a preferred **authentication method**, frictionless transactions supported by **risk-based authentication, merchant whitelisting**, impeccable user experience, all while being **fully SCA compliant.** As the 3D Secure 1 end of life is approaching in 2022, merchants and issuers will have to adapt to the new secure online payment environment, which will demand the use of 3DS2 across Europe.

To see what the future of online payment security holds, ASEE took a deep dive and handpicked the trends that will follow, as well as predictions for the upcoming years. The following pages provide insight into eCommerce and fraud forecasts, learn about the latest approaches when it comes to assessing security risks, and find out more about the latest authentication trends in the industry.

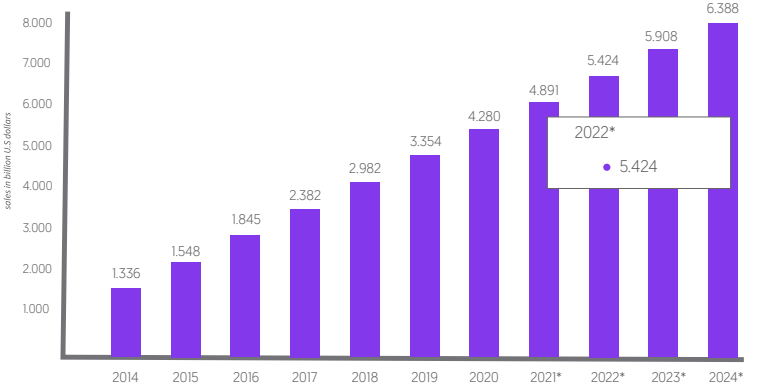
2. Rise in Online Payments Equals Rise in Fraud

It is no wonder that heightened online activity will result in an increase in fraud. To put things into perspective, we gathered information about past trends and forecasts for the upcoming years related to eCommerce and fraud. Both figures are marching in the same direction at a fast pace.

2.1 eCommerce and Fraud Forecast: Stats to Consider

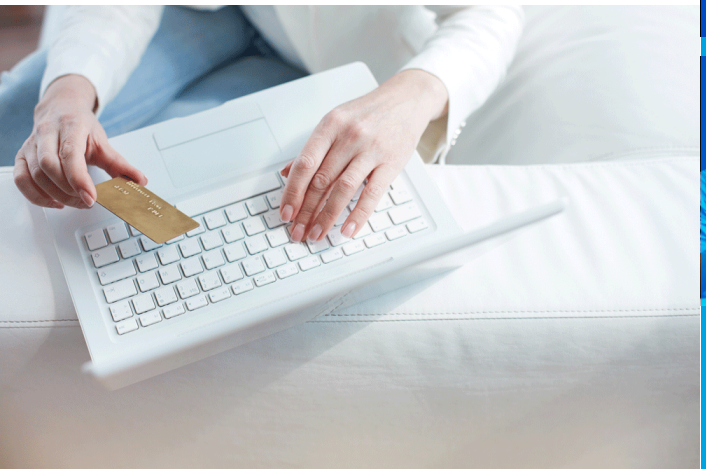
Projected figures for total eCommerce sales worldwide in 2021 are 4,891 billion USD, and 5,424 billion USD in 2022. This is an almost 10% y-o-y increase indicating yet another significant year for online payments growth. **If we take a look at eCommerce fraud statistics for 2021, analysts report that the global losses will amount to more than 20 billion USD,** which is an 18% growth from 2020 to 2021. This means that **20 billion USD worth of eCommerce sales turn out to be fraudulent transactions,** ending up as either chargebacks or completely lost funds.

Retail e-commerce sales worldwide from 2014 to 2024
(in billion U.S. dollars)



Another discouraging source regarding **eCommerce fraud states that eCommerce fraud losses will exceed 206 billion USD cumulatively for the period between 2021-2025.** Experts say the reason for such grim figures lies in the use of synthetic identities and the rise in account takeover fraud, which is one of the most common types of online payment fraud nowadays.

A big part of eCommerce sales is and will continue to be under the influence of the fast-growing mobile payments industry. According to **mordorintelligence,** in 2020, the mobile payments market was valued at 1449.56 billion USD. **The same figure projected for 2026 is 5399.6 billion USD at a 24,5% CAGR (compound annual growth rate) for the period between 2021 to 2026.** Merchants are quickly adapting to alternative payment methods and are rushing to integrate mobile payments into their business. Due to the convenience and accessibility of such services, mobile payments are here to stay, and the security of this channel will play a great part in eCommerce fraud statistics for the upcoming years.



2.2 Common Attacks to Look Out For

Among various online payment fraud, **Account takeover and Chargeback fraud have proven to be the most harmful to businesses and cardholders.**

Account takeover attacks are based on illicit access to a user's account followed by making unauthorized withdrawals and purchases. The problem lies in insufficient account protection in the form of simple usernames and passwords, which are oftentimes reused, even shared with friends and family members. Easy access to sensitive user information available on the dark web does not make things easier for security experts aiming to prevent malicious acts. **Estimated losses due to ATO fraud have cost businesses around 12 billion USD.** That is why we see more and more account-based websites and services turn to two-factor authentication as a necessary security measure.

Chargeback fraud also referred to as **friendly fraud**, is probably the most difficult one to detect at an early stage. The reason behind this is the fact that the person committing frauds is the actual cardholder or the rightful owner of an account, aiming to abuse the **chargeback** system. **The fact that 86% of chargebacks are considered to be the result of friendly fraud indicates that cardholders with malicious intentions have figured out how to game the system and do not plan on changing their bad habits.**

3. Improved Risk Assessment Through Machine Learning

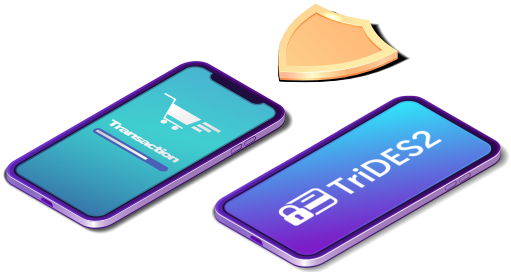
Rule-based risk assessment has proven to be effective so far, **but machine learning unlocks the full potential for fraud prevention and detection**. By running collected raw data through machine learning algorithms, you are generating intelligence that offers a much bigger picture. What makes machine learning so great is the capability to assess tremendous amounts of versatile data and easily extract risk scores with minimum manual effort.

Properly setup **risk scoring engines enable filtering out fraud scenarios that meet the previously defined criteria**. This approach implies the existence of a "normal scenario" to which all other transactions are being compared, leaving room for error. However, rule-based risk assessment is effective in detecting anomalies and deviations such as transaction amount, geolocation, and timezone mismatches. Another implication is the fact that **rule-based libraries keep expanding, putting a lot of pressure on the system as a whole**. The growing complexity of a rule-based solution tends to result in heightened rates for false positives and false negatives as well. But there is a solution to overcome these obstacles.

To maximize security and optimize system operations combine machine learning algorithms and rules. Look for a machine learning solution containing a variety of algorithms and choose the one that best suits your needs. Also, **consider combining supervised and unsupervised machine learning models. Supervised machine learning gives the best results when it comes to detecting known fraud, while unsupervised machine learning enables the discovery of new patterns and is capable of detecting evolving fraud.**

3.1 Mobile Payments Open Doors For Data Enrichment

For the past couple of years, we have witnessed financial companies knockoff their internet banking services on the mobile channel. **This breakthrough caused both new opportunities for fraud as well as access to a fresh set of data that can be used for risk assessment. Within mobile, gathered data is much more contextual and serves as a quality resource for further fraud prevention.**



Examples of common data that can be extracted from mobile devices include the device brand, operating system, installed version of the OS. But you can go so much further than that. You can analyze if the phone is connected to their normal wi-fi, if there are any Bluetooth devices connected, which type of keyboard is being used, default or custom, is the phone rooted/jailbroken. Also, mobile allows the assessment of behavioral factors, meaning how the user interacts with the device. What are the common features used within an app by the user? Is their typing speed deviating from the usual? At which angle is the user holding their phone?

By applying mobile data to machine learning, you are producing a number of quality inputs for further fraud prevention and detection development. Of course, to gather such data, you need a secure solution capable of collecting it. **3DS Mobile SDK** is a solution that is easily integrated within mobile applications offering secure in-app purchasing. Not only does it enable data enrichment, but it also helps with conversion rates and makes the checkout smooth and secure.

4. Customer Centricity in Online Payments

Although the trend of customer centricity has been around for a while, the Covid-19 pandemic has put this approach on a fast track. This is prominent in the financial industry by making payments fully digital and thus more accessible. **Forced digitalization of payments inevitably pushed banks and other financial institutions toward a more customer-centric business model.**

Being a part of such a volatile market, financial institutions need to adapt more than ever before to their customers. **With the amount of influence a single customer has, customer-centricity should be a part of their business strategy,** rather than a new phrase that everybody likes to throw around.

Sticking to default offerings without taking the time to hear out your customers is no longer an option. The competition is ready to overtake a portion of your clients by simply offering them what they asked for.

4.1 Mobile: The Pillar of Customer Centricity in Online Payments

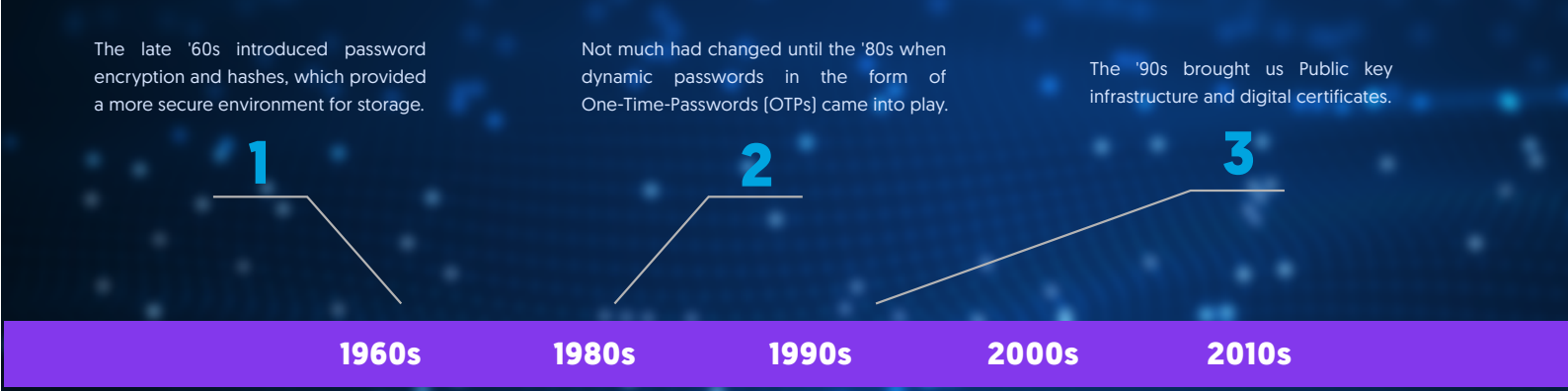
Customer centricity reflects on both quality of the product as well as the quality of customer service. **The product aspect nowadays tends to be tailor-made, personalized to the users' wishes and needs.** The development needs to consider delivering a solution that allows custom features for the individual.

Detecting your customer's needs requires a great amount of **market listening and unbiased in-house analysis.** Focusing your efforts on pinpointing issues within your business model that directly affect your customers is a key starting point. When it comes to online payments, two customer requests are present: **easy access to online payments and less friction.**

That is exactly what mobile provides to the customers and the reason why you should optimize for mobile. As mentioned, **the projected figures for eCommerce sales in 2026 coming from the mobile channel is 5399.6 billion USD.** Users love the convenience of mobile banking applications and in-app stores. They like to do things on the go, and mobile enables them precisely that, access to services ranging from online shopping to trading crypto during their daily commute.

5. Behavioral Authentication Revolutionizing Online Payment Security

Let's take a step back and see how authentication methods progressed over time.



trides@asseco-see.hr

5.1 Behavioral Authentication: Protection and Detection Combined

Static information and physical features are still used for accessing online services such as online and mobile banking applications. However, bad actors in the online payments scene are catching up, developing a necessity for even more robust security measures. **Behavioral authentication lives up to that hype.**

Behavioral biometrics focus on the user's interaction with the device being used for authentication. Regardless of whether the behavior analysis is applied for interacting with desktop or mobile applications, behavioral analytics are proving to be successful at filtering out fraudsters and bot attacks.

Common identifiers used for evaluation are the following:

01 **Device focused identifiers:**

At what speed is the user typing? Are they using shortcuts/advanced keys?
Are pressure and press size within the usual parameters?
At what angle is the user holding the phone?

02 **Device focused identifiers:**

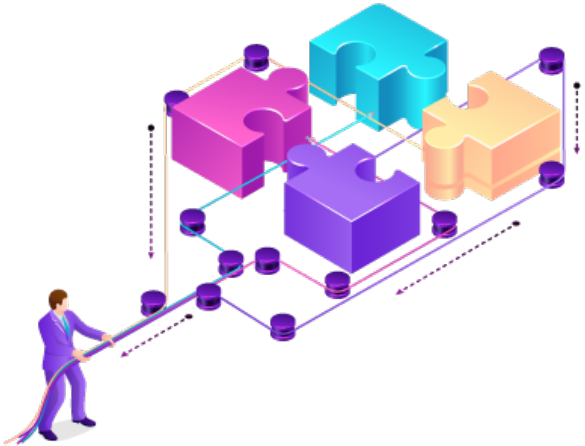
Are there any unrecognized Bluetooth devices connected to the smartphone?
Is the geolocation suspicious compared to the previous ones?
Is the user connected to their usual wifi?

03 **Service focused identifiers:**

At what time does the user normally use a particular online service?
What is the user's typical flow when unlocking their phone?
What functions within the app do they typically use?
Are there any deviations from how the user usually scrolls through an app?

There is no doubt that in the near future, such an approach will become standard practice. **By leveraging machine learning and behavioral authentication, you are getting one step closer to building a bulletproof security system** able to detect and prevent online payment fraud.

Wrapping up



Online payments went through an extreme makeover during the past couple of years. Along with 3D Secure 1 end of life approaching in the upcoming year, demanding Issuers to switch to the latest version of the protocol, there are other trends that follow this transition. Added accessibility and convenience brought underlying issues in the security sector that need to be addressed. Efficient fraud protection and detection are highlighted as a top priority for future development in online payments. Emerging technologies such as Machine Learning and Behavioral authentication are at the forefront when it comes to heightening security measures in this area.

The good news, simultaneous growth in mobile payments enables access to data that is more contextual, making a perfect candidate for data enrichment necessary to improve the accuracy of risk assessment. Moreover, customer centricity in the financial sector is going to play a significant role in keeping and attracting new clients since banking has become one of the most competitive sectors of today. **Investing your time and resources into research and development of the before mentioned trends promises to yield results and an increase in ROI.**

Sources:

Juniper Research
Statista
Mordor Intelligence
National Merchants

6. ASEE Group as your 3D Secure partner

With over **20 years of experience in authentication, payments, risk, and compliance solutions, we understand your needs**. Stacked with valuable know-how and skilled professionals in industries such as banking, payments and finance, we are a resourceful partner and a top-notch cybersecurity vendor to your company. **Payten**, part of the **ASEE Group**, provides **complete payment industry solutions for financial and non-financial institutions, as well as offering support for card and cardless transactions.**

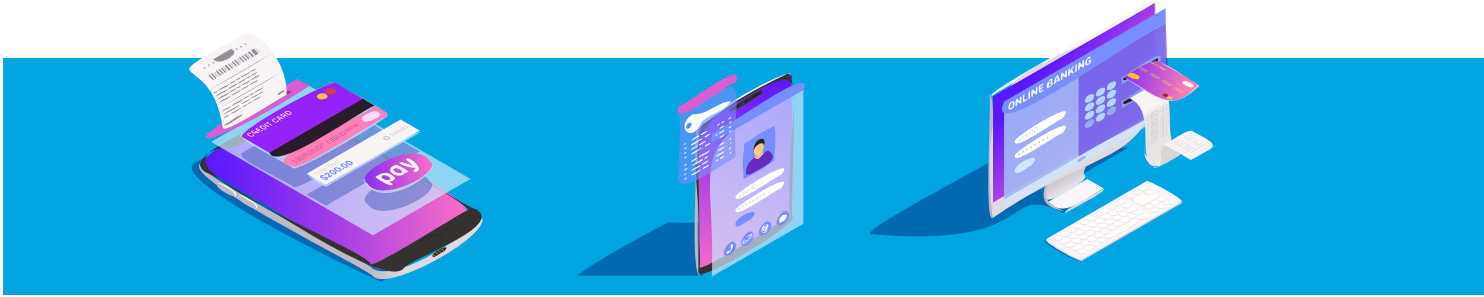
In case you have any questions regarding your **3D Secure journey**, we are happy to advise you and provide support along the way. To better understand what to expect from **3D Secure 2.0**, we are more than happy to showcase all the functionalities of the solution using our **3DS2 DEMO platform**.

ASEE GROUP FACTS & FIGURES:

- Top-notch **cybersecurity vendor**
- Serving customers across four continents, **20+ countries**
- **190+ Banks** in the client network
- End-to-end Product/Solution portfolio for banking operations
- Processes **+1B eCommerce transaction**s in a year
- Processes **+5.5M tokenization transactions** per month

TriDES2

asee by asseco



ACS, Access Control Server, enables Issuing institutions to participate in the 3D Secure program by ensuring that cardholder is authenticated during online CNP transactions. This is done through either Risk-Based Authentication or using the available authentication method such as One Time Password, SMS OTP, mobile token, or biometrics.

Risk Scoring Engine evaluates transaction risk based on information provided by 3DS Server and ACS. Depending on the level of transaction risk, online CNP ransactions are authenticated using either frictionless flow or by demanding an additional Strong Customer Authentication method.

3DS Server enables Acquiring institutions to provide 3D Secure protection to their Merchants. Simple integration with webshop or mobile application grants Merchants card scheme liability shift in cases of proven online payments fraud.

3DS Mobile SDK is integrated into mobile purchasing applications and enables Merchants to participate in the 3D Secure program, improving the checkout User Experience accompanied by data enrichment for more accurate risk assessment.

3dsecure.asseco.com

For more information, please contact us at **trides@asseco-see.hr**, and arrange your free, **zero-obligation consultation** with our team of experts.