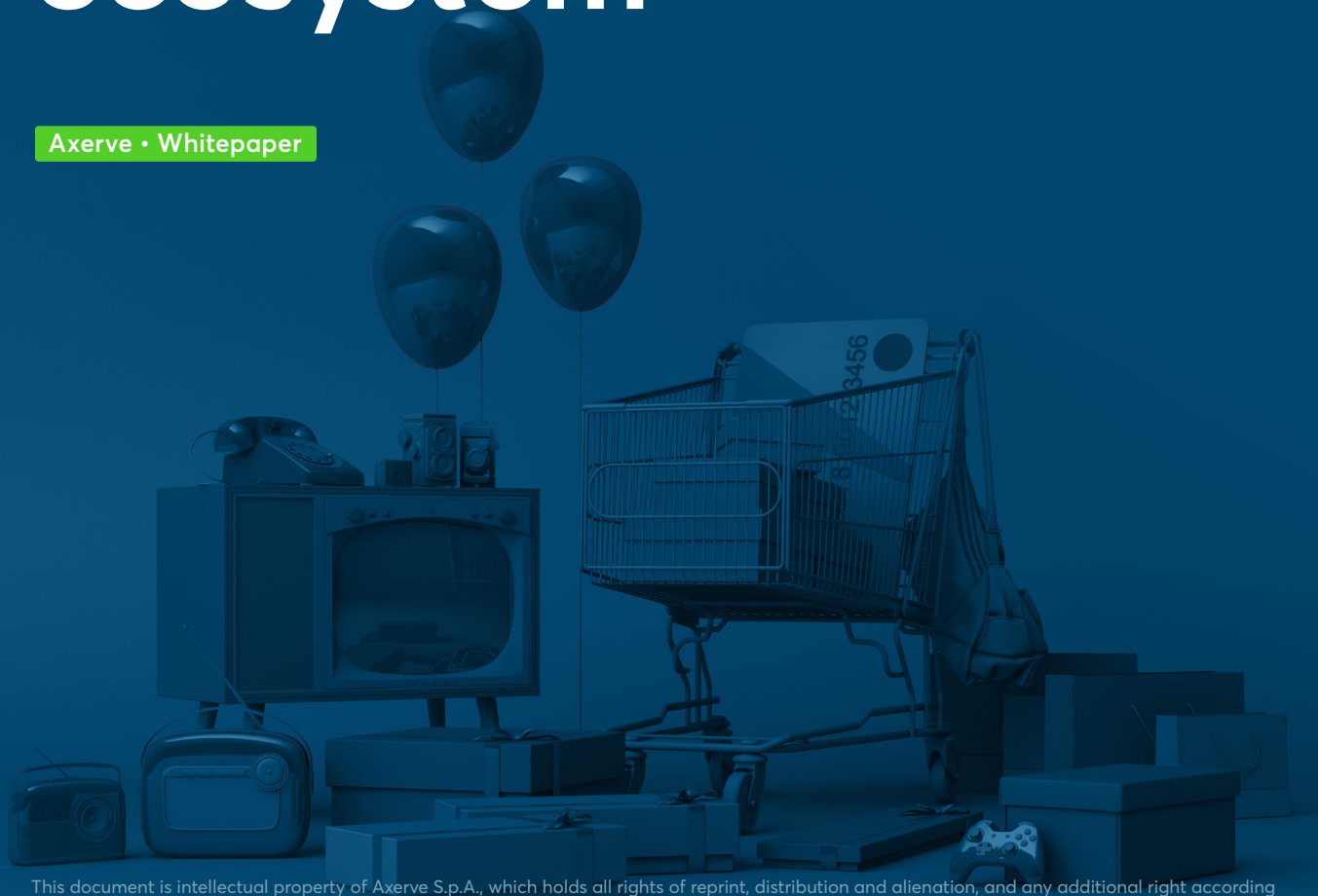
axerve

Your Payment Partner to Grow

Cybercrime and online fraud: a challenge for the entire Ecommerce ecosystem

Axerve • Whitepaper



Contents

Online scams and the impact on consumer's trust 3

Cybercrime in Europe 7

Online fraud in the UK 9

The techniques used for online fraud 10

Ecommerce fraud: how much they cost the entire industry and how to prevent them 16

Ecommerce fraud in Europe and the United States: the point of view of merchants and consumers 21

PSD2 and Strong Customer Authentication alongside the entire Ecommerce ecosystem 22

Risk analysis and artificial intelligence: Axerve's response to fraud 24

Axerve Guaranteed Payments: artificial intelligence at the service of fraud prevention 24

Axerve Advice: how to improve the conversion rate on authentications 25

Ecommerce and the Payment Orchestration revolution 26

Fraud Prevention and Payment Orchestration 26

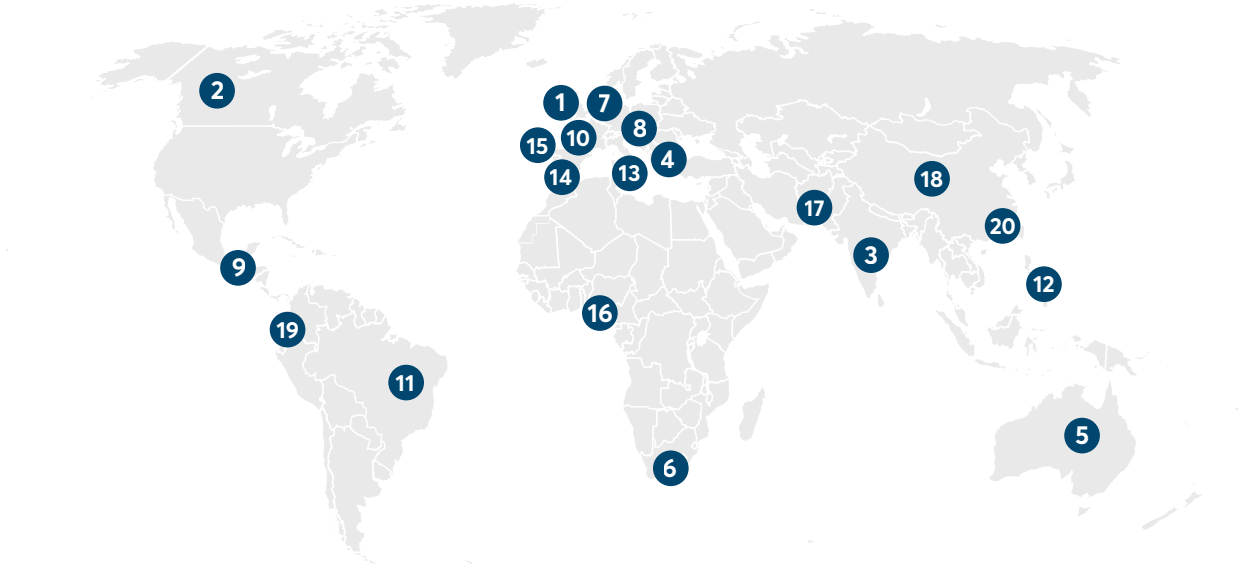
Sources 28

Online scams and the impact on consumer's trust

The advent of the internet has revolutionised many aspects of our life, not least that of purchases and, therefore, payments. At the same time since the beginning, the web has been fertile ground for telematic scams to the detriment of consumers and merchants. From fake merchants who, once payment is received, do not ship the goods to credit card numbers cloned or stolen from their legitimate owners, online fraud has grown over time, not only in terms of volume but also for complexity of threats and it continues to slow down the development of Ecommerce in the world.

Although over the decades the solutions to protect buyers and sellers have multiplied and evolved, Ecommerce is still not free from risks, also due to the increasingly sophisticated tools available to those who commit illicit acts. To contribute to the propagation of software and data necessary to perpetrate online fraud there is also the so-called dark web, that is the set of content and web resources, often illegal, accessible only through specific platforms and authorizations, where useful tools for criminal activities are traded.

According to the "Internet Crime Report 2020" published by the FBI Internet Crime Complaint Center (IC3), in 2020 alone the reports of online scams were almost 800 thousand, 69% more than in 2019, for a total value of 4.1 billion dollars.



Top 20 international victim countries

1. United Kingdom	216,633	**6. South Africa**	1,754	**11. Brazil**	951	**16. Nigeria**	443
2. Canada	5,399	**7. France**	1,640	**12. Philippines**	898	**17. Pakistan**	443
3. India	2,930	**8. Germany**	1,578	**13. Italy**	728	**18. China**	442
4. Greece	2,314	**9. Mexico**	1,164	**14. Spain**	618	**19. Colombia**	418
5. Australia	1,807	**10. Belgium**	1,023	**15. Netherlands**	450	**20. Hong Kong**	407

Source: Internet Crime

In the five-year period between 2016 and 2020, IC3 received a total of 2,211,396 reports for a total of 13.3 billion in losses to the detriment of companies and consumers. After the United States, which recorded 540,710 victims of online fraud in 2020, the most involved country in the world was the United Kingdom, which with 216,633 cases far exceeded Canada, which is in third place with 5,399 reports.

The IC3 report shows that in 2020 the three age groups most affected in the United States were those over 60 (105,301 cases of fraud that generated 966,062,236 dollars in fraud), followed by the 50-59 range (91,568 cases that caused losses of 717,161,726 dollars) and then the 40-49 range (85,967 cases, for a volume of 847,948,101 dollars).

2020 VICTIMS BY AGE GROUP

Age range	Total count	Total loss
Under 20	23,186	$70,980,763
20-29	70,791	$197,402,240
30-39	88,364	$492,176,845
40-49	91,568	$717,161,726
50-59	85,967	$847,948,101
Over 60	105,301	$966,062,236

It is therefore the older generations who are most affected. By analyzing the average losses, what catches the eye is that, although people over 60 are the age group with the highest number of those affected, it is the population between 50 and 59 years, third in the ranking for the number of frauds, that generated the higher average loss, with a value of around $ 9,864.

Figure 1 - Source: Internet Crime Report 2020

It comes as no surprise that the population most at risk is the one with less confidence in digital tools, easier prey than the so-called scammers who often use subtle practices to convince their victims to provide personal data. An example above all are telephone frauds, particularly suitable because they exploit a channel well known to the victims, followed by phishing e-mails through which personal data are stolen.
The data reported by IC3 does not represent the entirety of online scams worldwide, both because many are not reported or discovered and because there are a multitude of government bodies or organizations that are involved in collecting and investigating these phenomena, so data is fragmented.

Among these is also econsumer.gov, project of the International Consumer Protection and Enforcement Network (ICPEN) which, since April 2001, has been collecting and sharing reports of Ecommerce-related scams with Member States. This initiative forms a web of government

organizations of more than 40 nations that fight for the enforcement of laws on fair trade practice and other consumer protection activities.
The cross-border reports collected by econsumer.gov, which collaborates among others with the US Government Agency for Consumer Protection (Federal Trade Commission) and with the Italian Competition and Market Authority (AGCOM), have drastically increased from 2017 to date, as has the economic damage generated by the scams related to them.

In 2017[1] the reports received by econsumer.gov were 19,545, 77% of which actually generated losses for a total of over 73 million dollars. However, already by the end of 2020 the complaints collected had risen to 60,835 and as many as 85% have generated economic damages, for a total of 211.6 million dollars.

Data recently published by the Federal Trade Commission[2] on the American market offer an insight into online fraud in the United States.
They have always been pioneers in the electronic commerce sector and therefore are a point of reference to identify possible global trends in advance.

In the timeframe between the 1st January 2020 and 5th August 2021 - therefore in the middle of the pandemic period - the total of frauds recorded by the FTC was 347,945 for a total of 519.43 million dollars and an average loss of 376 dollars. As can be seen from graph 2, most of the illegal activities are definitely related to online shopping and associated activities.
Only in 26% of the reports the contact channels used by the attackers were specified and in 37.3% of the cases the payment method used to finalise the transaction was noted. From the graphs published by the FTC, e-mail is at the top of the ranking of the most used communication channels but it is websites and apps that have generated the most profitable fraudulent revenues, recording a total of 46.06 million dollars in losses.

1 - econsumer.gov Internationa Fraud Report
2 - FTC COVID-19 and Stimulus Report

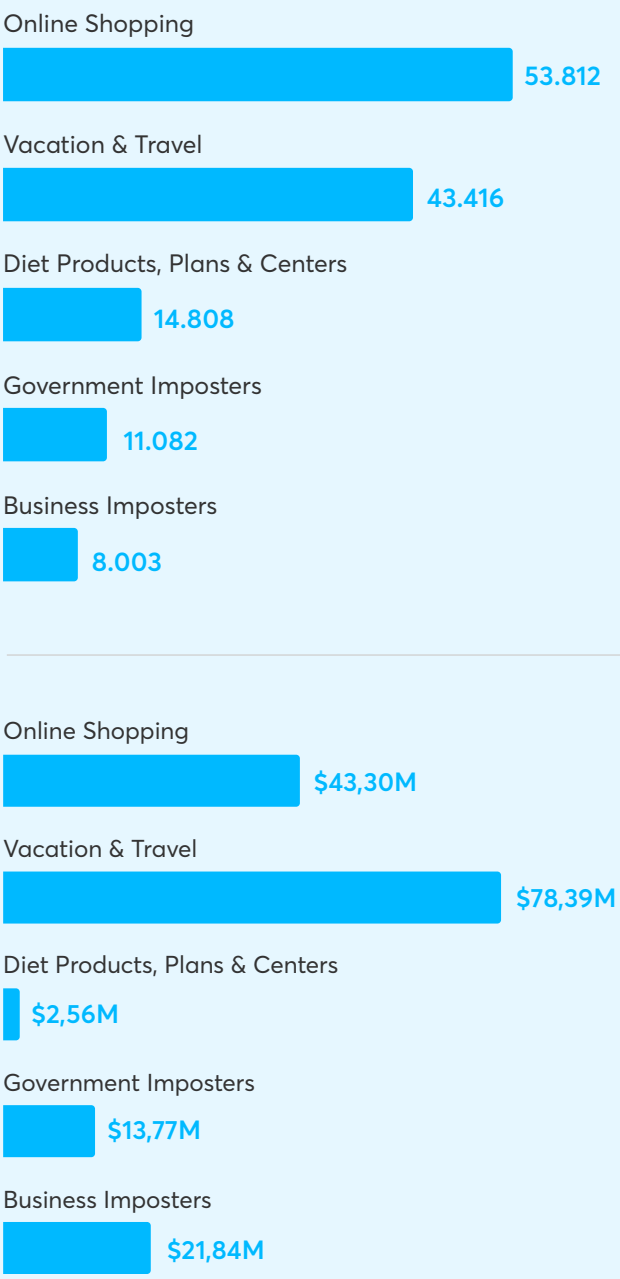
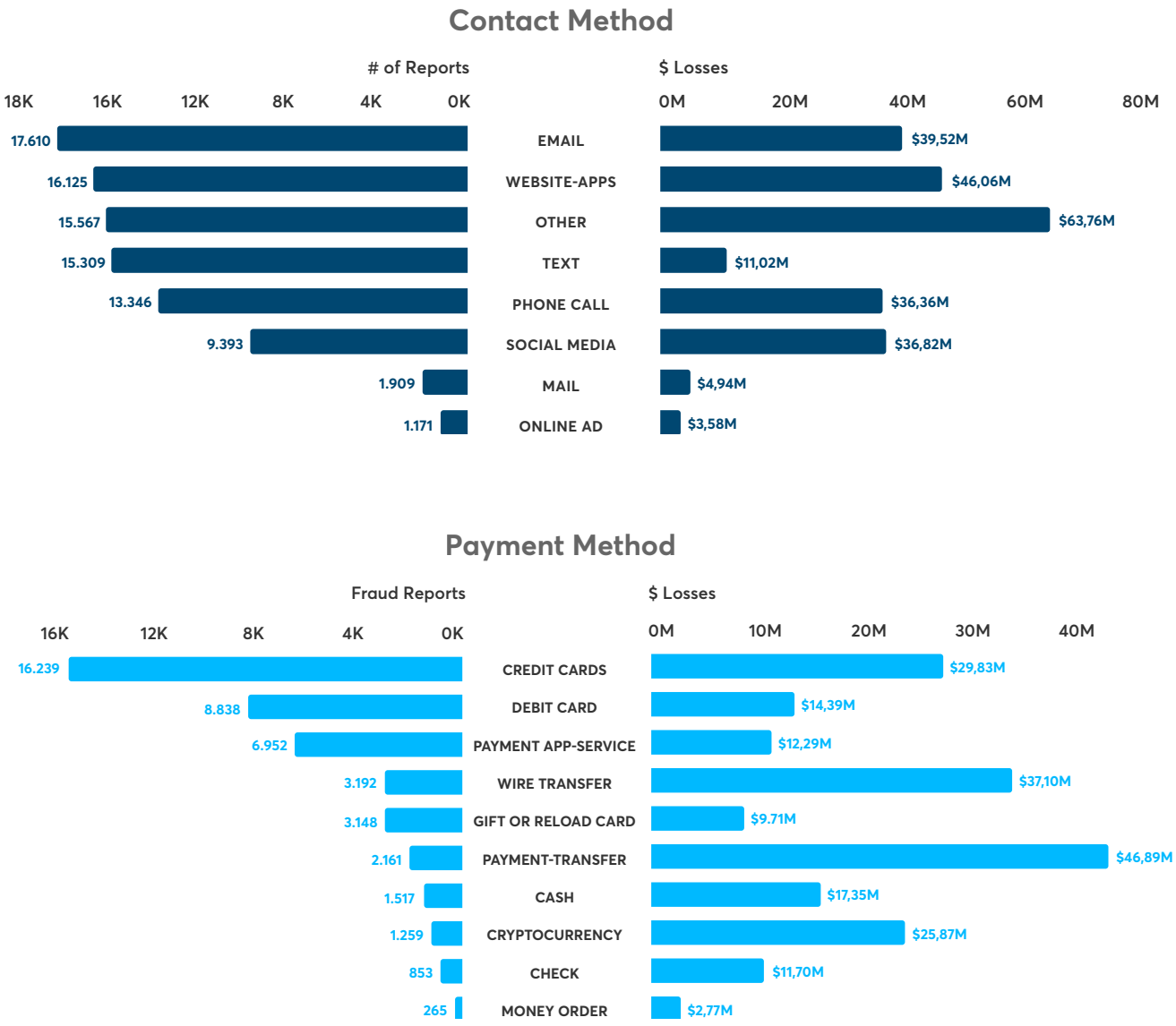


Figure 2 - Source: FTC COVID-19 and Stimulus Reports

Figure 3 - Source: FTC COVID-19 and Stimulus Reports



The largest volumes of losses were generated by a set of contact tools not attributable to the main channels specified in the search - which were identified as "other". These reached a volume of 63.76 million dollars in the period under consideration.

If we analyze the payment methods, it is credit cards that reach the highest number of reports (16,239), but in terms of the total amount, transfers (46.89 million dollars) and wire transfers (37.10 million dollars) far exceed them.
It is interesting to take a look at the average value of scams aimed at crypto-currencies which, compared to the 1,837 dollars of credit cards, rises to 20,548 dollars. However, we need to take into consideration the high volatility of the countervalue of these methods and therefore the quotations should be examined in depth during the data collection phase.

Cybercrime in Europe

The European Union is also stepping up and increasing the efforts to fight cybercrime. The joint communication to the European Parliament and Council "The EU's Cybersecurity Strategy for the Digital Decade" recognised cybersecurity as an integral part of the security of the Union: whether it is connected devices, banks, public administrations or hospitals, the entire population has the right to use services with the security of being protected from any digital threats.

According to the European Union, economy, democracy and society all depend on safer and more reliable tools and connectivity that are also essential for building a resilient, eco-sustainable and digital Europe.

"Europe is determined to carry out a digital transformation of our society and economy, which we must therefore support with unprecedented levels of investment. The success of the digital transformation, which is accelerating, is based on citizens' and businesses' confidence in security of the related products and services they use."

Margrethe Vestager, Executive Vice President of the European Commission for A Europe Fit for the Digital Age[3]

Data published by GSMA[4] - the organization representing the interests of 750 mobile network operators and 400 companies in the sector worldwide - confirm that by 2025 the Internet of Things (IoT) will see over 25 billion connected devices that will be able to generate an economic potential of over 1.1 trillion dollars, 242 billion of which only for the European market. These numbers represent great opportunities for the Ecommerce sector and, at the same time, for criminal organizations around the world.

"Cyber-security is a central element of the Security Union. There are no longer distinctions between online and offline threats and the digital dimension is now inextricably linked to the real dimension."

Margaritis Schinas, European Commissioner for Promoting the European Way of Life[3]

Despite the efforts of all institutional bodies and private companies of the security sector in the fight against cybercrime, European citizens still show distrust of the digital ecosystem, especially in terms of data management. This is what emerges from "Crime, safety and victims' rights"[5], a study published in February 2021 by the European Agency for Fundamental Rights (FRA) and based on a survey carried out in the 27 countries of the Union, the United Kingdom and North Macedonia, in the period between January and October 2019, which involved about 35,000 respondents.
In the research, which includes some questions related to consumer fraud on credit cards and online banking, it appears that 8% of European respondents have experienced at least one online fraud in the past 5 years, which drops to 3% if we use as a reference the 12 months prior to the interview. The data from the research is actually variable and ranges from 1% to 19%, probably also due to the different penetration of these services in individual Member States.
A significant difference comes out in the comparison between people with health problems

3 - New EU cybersecurity strategy and new rules to make physical and digital critics more resilient, European Commission
4 - The Internet of Things by 2025, GSMA
5 - Crime, Safety and Victims' Rights, European Union Agency for Fundamental Rights

or disabilities and the rest of the population: 14% of the first category say they have suffered a scam of this type in the previous 5 years, against 6% of the rest of the respondents.
26% of European consumers declared that they had suffered at least one fraud as a consumer on either quantity, quality, price, shipment of goods or provision of services in the five years preceding the survey, a figure which drops to 16% if we only look at the last year before the investigation. As in the previous case, the information collected is highly variable depending on the country of origin, in fact the results vary from 8% to 46% depending on the geographical region.
When describing the most recent incident of fraud suffered, 41% confirmed that they had purchased goods or services online, by phone or by mail from a foreign site or company, which was much higher for some countries such as Luxembourg (94%) and Malta (87%).

Almost all the European citizens involved reported scams related to the use of online banking services and credit card fraud to the competent orders,

Reporting the most recent incident of three property crimes asked about in the survey (EU-27, %)

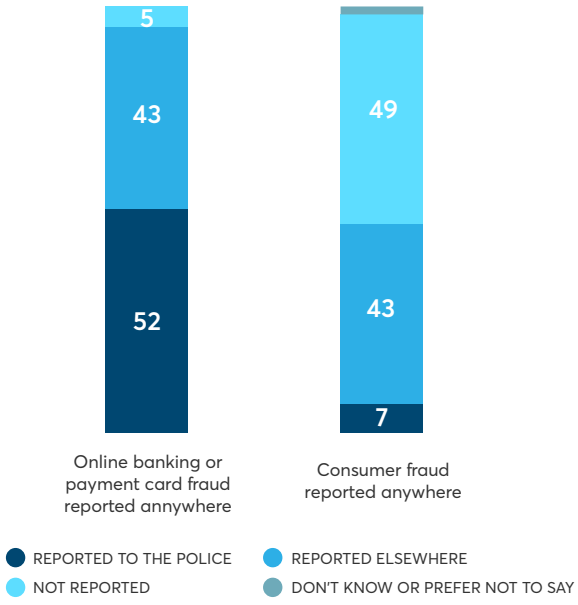


Figure 4 - Source: Crime, Safety and Victims' Rights, European Union Agency for Fundamental Rights. Data collected in collaboration with CBS (NL), CTIE (LU) and Statistics Austria (AT)

some to the Police (52%) and others to other channels (43%), while only 5% have preferred to abstain. 50% of consumer frauds were reported (7% to the police and 43% to other bodies) while the remaining 49% preferred not to report.
The number of responses related to the most recent frauds is highly variable, the values of which were recorded, for example: Portugal (69%), France (65%) and Germany (60%) with higher volumes than Greece (25%), Croatia (28%), Slovenia (29%) and Sweden (30%).

According to the people involved, the deterrent is often the cost of a possible litigation due to the lack of economically sustainable procedures of judicial systems and economic resources for the protection of consumers. Not only that, the reasons for the failure to report fraud against the consumer were also other ones:

- 49% considered what happened of little importance;
- 25% gave up, in the belief that the complaint would have served no purpose.
- While regarding the scams suffered on credit and debit cards or through online banking:
- 22% considered the seriousness of what they suffered to be almost irrelevant;
- 22% said they failed to report due to lack of evidence;
- 21% did not report because they personally took care of managing the incident;
- 28% stated other reasons than those foreseen in the survey.

The survey by the European Agency for Fundamental Rights therefore reveals a picture of uncertainty for citizens. Moreover, at least a quarter of the people involved believe it is of little use to report illegal activities in the field of payments as consumers, showing in fact little trust in the tools made available to the public.

Online fraud in the UK

The topic of online fraud is extremely relevant all over the world, both for its economic impact and for the national security law. The Data Protection Act 2018 ("DPA") covers general processing of personal data in the UK, while Network and Information Systems Regulations 2018 ("NIS Regulations") concerns cybersecurity in the country. Since Brexit, the UK is now a "third country", which means that some of the current mechanisms used in the EU have changed for the UK. Now it is up to the UK whether to adopt wholly or in part the updated NIS Directive for the EU members. In April, 2021, the government announced its plans for new cybersecurity legislation in the UK to protect consumer smart devices, including phones, TVs, wearables, toys etc. All the devices that fall under the category of the Internet of Things.

To explore the subject further, there are the following documents to look into: the UK Government's Code of Practice for Consumer IoT Security and the European standard EN 303 645 that goes into detail about Cyber Security for Consumer Internet of Things. Main takeaways for merchants are the banning of universal default password to ensure security, implementing means to manage reports of vulnerabilities, and telling consumers upfront how long a product will be guaranteed to receive security updates.

The annual value of Ecommerce fraud losses on UK-issued debit and credit cards in the UK grew from £28 million in 2002 to £376.5 million in 2020 with the peak in 2018 with £393.4 million. Even though after the Great Recession in 2009 there was a significant drop in Ecommerce fraud losses that lasted 4 years with an average loss of £142 million per year. Still, there were almost 3 million fraud actions related to cards in 2020 in the UK alone[6]. Online shopping and auctions fraud reported to the police increased by three times during the pandemic and became the most common type of fraud reported to the police in the UK. Axerve published an insight on online payment fraud, where the situation in the UK and worldwide is looked into even more in detail.

The UK National Cyber Security Center (NCSC) declared in May, 2021 that online scams increased by 15 times during the pandemic period in 2020-2021 in their annual report on Active Cyber Defense (ACD) programme, you can get familiar with it by downloading the report from the public sector information NCSC website. Some of the report's highlights: UK government phishing regarding Brexit was low, but there were still more than 11,000 government-themed phishing campaigns in 2020 that were successfully stopped by NCSC. Also, interestingly, the most phished UK government department in 2020 was Her Majesty's Revenue and Customs. Another brand-new service performed by ACD that had a particular boom in reports in 2020 was Suspicious Email Reporting Service thanks to being shared on social media. And just in the first 30 days (late April - late May 2020) the service received over 500,000 reports. And by December 31, 2020 the public sent almost 4 million reports, which amounts to almost 16,000 a day.

A national fraud unit in the UK also arrested more than 150 fraudsters since the beginning of the pandemic, and more than 2,000 websites were taken down. The City of London Police reported that incidents of online shopping fraud increased by 42% since the UK lockdown till March 2021. However, computer software service fraud decreased by 15.5%, which testifies for shifting priorities among fraudsters due to the pandemic, more towards the cybercrime and online fraud, like in most countries.

6 - Fraud - The facts 2021, UK Finance

The techniques used for online fraud

Among the difficulties encountered by those involved in fighting the phenomenon of online fraud is the growing commitment of all the actors involved to keep up with the continuous evolution of the tools used to perpetrate these illegal acts. Below, we have collected some of the most used techniques, with analytics and scenario insights.

Account Takeover

The term account takeover (ATO) refers to the fraudulent practice of theft of a person's online identity to obtain profit, by making purchases online or for other criminal activities, to the detriment of consumers and companies.
According to an analysis carried out by Sift[7] - company that deals with payment fraud prevention - the account takeover attempts of their network grew by 282% between the second quarter of 2019 and the same period of 2020.
Further confirming the relevance of these attacks is a recent research published by Arctic Wolf[8] - company operating in the corporate security sector – which, by analyzing the data of the first six months of 2020, found a 429% increase in credentials exposed on the dark web and a 64% increase in phishing and ransomware cases in the second quarter, comparing the two quarters of the same year.

Authorised Push Payments (APP)

Even the fraudulent activities related to Authorised Push Payments (APP), i.e. when the victim is enticed to send money to the fraudster, generate significant volumes. In 2020 only in the United Kingdom, according to the banking association UK Finance[9], these attacks cost 479 million pounds, respectively 387.8 million to the detriment of consumers and 91.3 million paid by companies.
According to GBG[10], a company that operates in the field of data intelligence and fraud prevention, these activities are particularly effective and could become the most significant online threat of 2021, further affecting corporate balance sheets.

Malware

Malware are programs typically shared as attachments via e-mail or saved on memory media (e.g. USB sticks, portable hard drives, etc.) which, once opened, give access to the user's devices, from which confidential data is stolen to then be used for illegal purposes, such as unauthorised payments.
SONICWALL - company specialised in cybersecurity solutions - has carried out a research[11] on the main online threats where malware is decreasing. Attacks recorded in the first half of 2021 amounted to 2.5 billion, which for the first time in ten years of monitoring gets the number down by 22% compared to the same period of the previous year. In 2010, the volumes were 8 billion and in 2018 they reached a maximum of 10.5 billion attacks, before falling to 5.6 billion in 2020.
Despite the decrease in malware threats globally, the study found a 23% increase in Asia. North America and Europe had a decline of 25% and 13% respectively, with the exception of Germany which recorded an anomalous increase of 465% in the first part of the year.

Pharming

With the word *pharming*, a neologism that comes from the union of the words phishing (a technique for acquiring personal data which we will discuss

7 - Digital Trust & Safety Index: Account Takeover Fraud and the Growing Burden on Business, Sift
8 - Security Operations Annual Report, Arctic Wolf
9 - FRAUD – THE FACTS 2021, UK Finance and LexisNexis
10 - GBG Fraud Survey 2020, GBG
11 - 2021 MID-YEAR UPDATE CYBER THREAT REPORT, SONICWALL

later) and farming (cultivate), we refer to the illegal activities carried out to access personal and confidential information of users who, unknowingly, access clone sites that are very similar if not identical to the original ones.
The pharming activity can take place thanks to the installation of a virus on the user's device or through fraudulent access to the Internet provider's DNS servers. In both cases the user, while correctly typing the address of a site such as that of his own bank, lands on a clone website from which whoever implemented the scam can steal information, like for example the access data to internet banking services or payment card numbers and codes.

Phishing

The phishing technique consists in sending an e-mail in the name of a company - typically a bank or an Ecommerce site - whose contents seem to all intents and purposes attributable to the sender. However, in this email confidential data is requested, which will then be used for: money transfers, online purchases or illegal activities such as selling stolen data on the deep web or requesting a ransom.
In some cases, the e-mail contains a link that lands on a cloned page of the company that is also the victim of the scam - for example a bank - to make the communication and legitimacy of the request even more credible.
The best-known use case is when access data to banking and financial services is stolen and criminals are able to make money transfers in their favor. In other cases, the credentials are stolen to access an Ecommerce site from which purchases are then made with the payment instruments saved by the user, not before having changed recipients and shipping addresses.
Data published in March 2021 by Trend Micro12, an American-Japanese multinational of cybersecurity software, shows that in 2020 their cloud-based services identified and blocked more than 16.7 million threats via e-mail, equal to 32% more than the previous year. Of these, 5,465,969 are attacks attributable to phishing activities which increased by 14% compared to 2019.

12 - Trend Micro Cloud App Security Threat Report 2020, Trend Micro

Credential phishing attacks

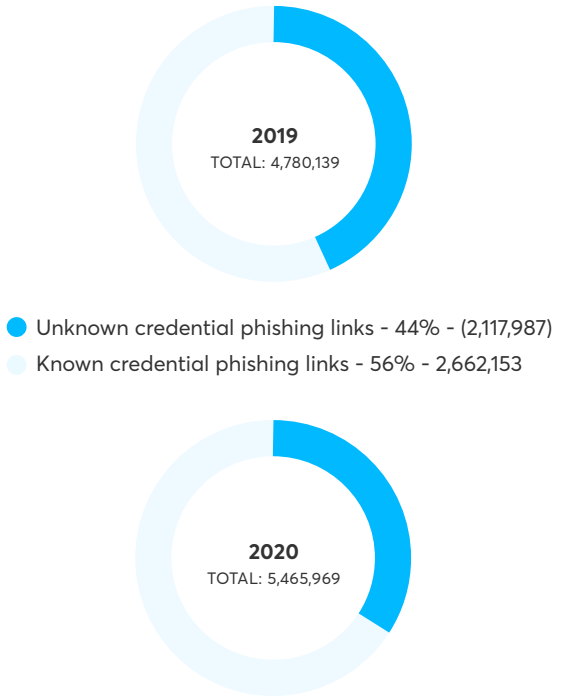


Figure 5 - Source: Trend Micro Cloud App Security Threat Report 2020, Trend Micro

Also due to the increasingly frequent use of smart working in many companies, other fraudulent techniques are performed through phishing attacks, such as BEC (Business Email Compromise) attacks. Similarly, to what happens in the cases of APP described above, in these cases the cyber-criminals send e-mails in the name of managers or top figures of the company to other employees and, thanks to the ability to make these communications indistinguishable from the authentic ones, they persuade them to make payments or money transfers in favor of current accounts in the name of third parties like suppliers, but, in reality, attributable or accessible by the criminals themselves.
According to a recent document by Mimecast[12], company that operates in the field of cybersecurity, in 2020 e-mail threats grew by 64%, also encouraged by the peak adoption of smart-working, and clicks on unsafe links with the advent of the pandemic reached 300% compared to the previous period. The data requires deep reflections

on the part of the entire ecosystem, especially if we consider that 13% of the companies involved in the research do not have a security system for e-mails and that only a fifth have provided in-depth courses for their employees on the subject of cyber security.

Ransomware

A ransomware, a word made up of ransom and malware, is a software that, once installed on a device, allows access only to the person who created the scam. Subsequently, the victim is asked for a ransom in order to be able to get hold of his data again.

This phenomenon is constantly growing: according to a report published by Cybersecurity Ventures[13], from 2021 to 2031 the increase in these activities will be equal to 30% year on year, reaching the level of one ransomware every 2 seconds within 10 years and a cost for businesses and consumers of $265 billion.

The Internet Crime Complaint Center in 2020 alone recorded 2,474 complaints for a total of over $29 million in losses[14]. It should also be considered that many of the people involved in this type of scam do not report either due to lack of confidence in the outcome of the investigations or because they are wary of releasing personal data, which are essential to identify the incident.

SIM Swapping

SIM swapping, also called SIM swap, consists in obtaining access to the telephone number of one or more users for illegal purposes. In particular, the intent of practice is to be able to carry out 2FA authentication (two-factor authentication) and then access services or make payments in place of the legitimate owner.

Those who carry out this type of attacks collect as much data as possible of the target person, for example through social engineering activities, and then ask the telephone operator to replace the SIM due to loss, impersonating the victim.

The European Police Office (Europol) recently stated that the SIM swap phenomenon is growing[15], also in the face of the fact that two-factor authentication is increasingly required by online platforms, such as social networks and platforms of crypto exchange.

The volumes attributable to these relatively recent events are difficult to quantify on a global level, but to get an indicative picture it is possible to refer to the press releases of the European police office. In February 2021, Europol itself declared that it had contributed to the arrest of ten hackers suspected of having stolen cryptocurrencies for an indicative value of 100 million dollars through the use of this technique[16].

A little less than a year earlier, in March 2020 to be precise, the same agency in collaboration with the Spanish, Romanian and Austrian police bodies, had communicated the arrest of dozens of members of different groups of people who generated illicit profits for over 3 million euros[17].

SMSishing

SMSishing differs from phishing in the communication channel. In the first case it is always e-mail while in the second one text messages are used. If you consider that in Italy, in the last 3 years, the use of text messages has grown 35%[18] despite the well-established use of alternative messaging platforms such as Whatsapp, Telegram or Signal just to name a few, it is easy to understand the potential this channel has for those with criminal intentions.

What makes this channel particularly attractive for scammers is the open rate of text messages which exceeds 93%, numbers well above those of e-mails which, although very variable depending on various factors such as the quality of the database, the time of sending or the effectiveness of the object, are well below those of text-messages.

It is good to keep in mind that SMS is the most

13 - The State of Email Security Report, mimecast
14 - Global Ransomware Damage Costs, Cybersecurity Ventures
15 - COVID-19 sparks upward trend in cybercrime, Europol
16 - Europol: 10 held for alleged $100m cryptocurrency theft from celebs, others, Reuters
17 - The SIM highjackers: how criminals are stealing millions by highjacking phone numbers, Europol
18 - Mobile Messaging Adoption Report 2021, Esendex e PricewaterhouseCoopers (PwC)

common instant communication tool for an audience that has less digital culture and therefore becomes more attractive for digital criminals.

Vishing

It is the practice that consists of a telephone call by someone who is pretending to be an operator of a company, often a bank, and asks the victims for some personal data useful for finalizing a scam, typically an outgoing bank transfer from the victim's current account. The phone call can often be followed by the sending of a phishing e-mail, in many cases justified by those who are calling to overcome the insecurity of the victim who prefers not to provide personal data over the phone.

This technique is targeted not only at the deception of consumers but also that of company employees. It is not uncommon for unsuspecting employees to install new company software that turned out to be malware through phone calls apparently coming from an internal office - typically the help desk.

In 2020 alone, IC3's activities[19] related to pharming, phishing, smsishing and vishing generated a loss of over $54 million. However, there are also new media and tools that are gaining positions in the ranking of the most frequent threats, exploiting platforms increasingly used by online users.

Malicious APP

When it comes to optimizing access to services via mobile devices, companies often choose to develop an app. Unfortunately, the proliferation of legitimate applications is accompanied by that of malicious apps that can be clones of other apps or simply applications with criminal purposes; in both cases their purpose is solely to steal the personal data of the user.

According to the latest quarterly report by Outseer[20], an RSA company that deals with security globally, 63% of all fraudulent transactions were generated by mobile and 47% of these occurred via app. Not only that: the increase in transactions is also accompanied by an average increase in the value of these payments (17%), a sign that the illegal activities carried out have increased their effectiveness.

Fraud transaction distribution by channel

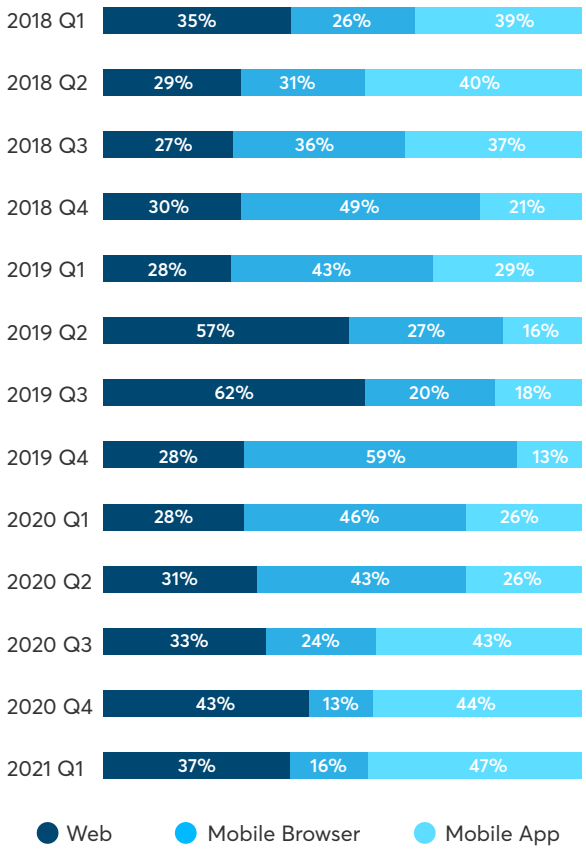


Figure 6 - Source: Q2 2021 Outseer™ Fraud & Payments Report, Outseer (RSA)

Social Media

Social media are the digital platforms on which online users spend most of the time: 145 minutes a day around the world. This is one of the reasons why they are an inexhaustible source of information that can be used to perpetrate online scams; being platforms where people share a lot of information, often personal, the risk is that it can be used for illegal activities related to identity theft through social engineering techniques, i.e. the collection and analysis of data of users to study their behavior and, in some cases, carry out illegal acts to their detriment or in their name.

19 - Internet Crime Report 2020, Internet Crime Complaint Center (FBI)
20 - Q2 2021 OutseerTM Fraud & Payments Report, Outseer (RSA)

According to the aforementioned RSA report[20], the cases of Brand Abuse, i.e. the set of fraudulent activities that exploit the name of a Brand without its knowledge, were over 28,000 in the first quarter of 2021 alone (56% of all attacks identified by Outseer), up from 27% in 2020. According to RSA, the increase in these threats is mainly attributable to the intensive use of social media in the most intense periods of the pandemic.

A PwC survey[21] that involved 3,249 executives in the business and IT sectors of international companies allows us to have a deeper insight the future of cyber-security in the corporate environment.

About 96% of the companies involved said they had to change their cybersecurity strategy due to the pandemic and 50% confirmed that they consider cybersecurity aspects in every business decision. In many cases, awareness of security has increased: 44% of respondents identified new budgeting processes for spending on security and quantifying risks and 43% increased comparisons between CISO and CEO and resilience tests, to obtain a lower probability of suffering high impact events.

55% of respondents predicted an increase in the dedicated budget for 2021:

- 8% have planned an increase in spending of more than 10%;
- 22% have budgeted costs that will be between 6% and 10%;
- 25% will spend up to 5% more.

13% of the companies affected by the survey will keep the same cyber-security budget while 27% will reduce investments in this area. Only 5% have not yet made decisions about how much to allocate for this sector.

The areas of expenditure declared by the executives interviewed are various and can be summarized as follows:

- People and hard skills
- Capabilities and processes
- Technologies
- Architecture
- Automation

21 - 2021 Global Digital Trust Insights, PwC

Particularly important is the transition to the cloud of operations (75% of respondents) and security (76% of respondents), both to reduce internal friction and to simplify the access of their customers to products and services.

The data emerging from PwC's research is in line with what emerged from a Gartner survey[22] which in September 2020 involved some companies on the subject of information security. The survey revealed that 67% of the companies concerned intend to increase the amount previously allocated by about 7% to protect their systems from online attacks, focusing in particular on artificial intelligence. Ultimately, the issue of online security is central and increasingly an integral part of the strategies of all companies globally, regardless of the size and product sectors in which they operate. Although awareness and investments on these issues are constantly growing, how much and how does the damage caused by online fraud affect the economic accounts of Ecommerce?

22 - 2021 Gartner Board of Directors Survey, Gartner

Ecommerce fraud: how much they cost the entire industry and how to prevent them

The global Ecommerce sector has grown over the past year and a half, with the exception of some offline industries due to restrictions imposed by many governments to deal with the pandemic, such as tourism and catering, for example. Many sources confirming this mostly positive trend in online sales were recently enriched by the "June 2021 Global Consumer Insights Pulse Survey"[23] conducted by PwC, which in March and then in June of this year interviewed 8,600 consumers from 22 countries.

Channel Choice

	MARCH '21	JUNE '21	GAP
Physical stores	42%	46%	9,50%
PC	30%	34%	13,33%
Tablet	33%	38%	15,15%
Smartphone	39%	44%	12,82%
Voice assist.	37%	42%	13,51%

Table 1 - Source: June 2021 Global Consumer Insights Pulse Survey, PwC

The respondents' purchasing channels preferences were collected in the report and it emerged that, with regard to online spending, tablets and voice assistants were subject to greater acceleration than computers and smartphones.

Over 50% declared that they considered themselves a more "digital" buyer compared to PwC's surveys of past years. Therefore, it is now strategic to invest in safety, integrating the results obtained in the latest period in the sector, while building customer loyalty. Customers, in turn, found themselves forced at that moment to rely on payment instruments considered unsafe, even if only for simple distrust and not objective security standards.
As we have seen, consumers' insecurity in reality cannot be traced back exclusively to prejudices or lack of knowledge. In fact, although better security is in the center of attention of the strategies of all companies that operate online, as we will see later, the costs related to prevention, and losses generated by illegal online activities continue to grow, weighing heavily on both merchants and their customers.

So how much does online fraud cost the merchants? It is difficult to accurately quantify the losses suffered by merchants globally, and there are many reasons for this. First of all, there isn't one shared database by merchants or acquirers. Secondly, the payment systems solutions available in the world right now are very fragmented, and keeping track of all the illicit activities recorded by each individual instrument and by all the PSPs is not a viable path today.
However, it is possible to analyse some research carried out precisely in the field of online payments to trace the perimeters, even if only indicative, and draw a general framework from which to set up conscious business choices in terms of safety and prevention.

FIS, an international player in the field of payment systems, has recently published the results of a survey commissioned to Forrester Consulting, in which nearly 700 managers of large Ecommerce

23 - The global consumer: Changed for good, PwC

companies participated from 11 countries around the world[24]. The research discovered that almost 90% of the interviewed companies suffered losses due to online payment fraud and about half of the companies spent on prevention from 1% to 5% of profits in 2020 alone.
According to the FIS survey, in 38% of cases the losses correspond to at least 6% of the revenues, to which the costs of the solutions implementation related to prevention and regulatory adjustments need to be added (the PSD2 regulation for example).

As highlighted in figure 7, the challenges that required the greatest effort were the costs associated with the IT updates and the security integrations, such as tokenization and the management of 3DS2 protocols.
One in four merchants considered the integration of fraud prevention solutions as particularly challenging, in addition to great efforts made in the areas of access to payments data and compliance with the newly introduced regulations.
At the top of the list of points of attention that characterised 2020 for the European companies interviewed, there are PSD2 and tokenization (28% of respondents). 27% of North American managers have identified the integration of security systems as one of the most important challenges of 2020, and the number reaches 30% in the South American market.

What are the top payment challenges that your team faced in the last 12 months?

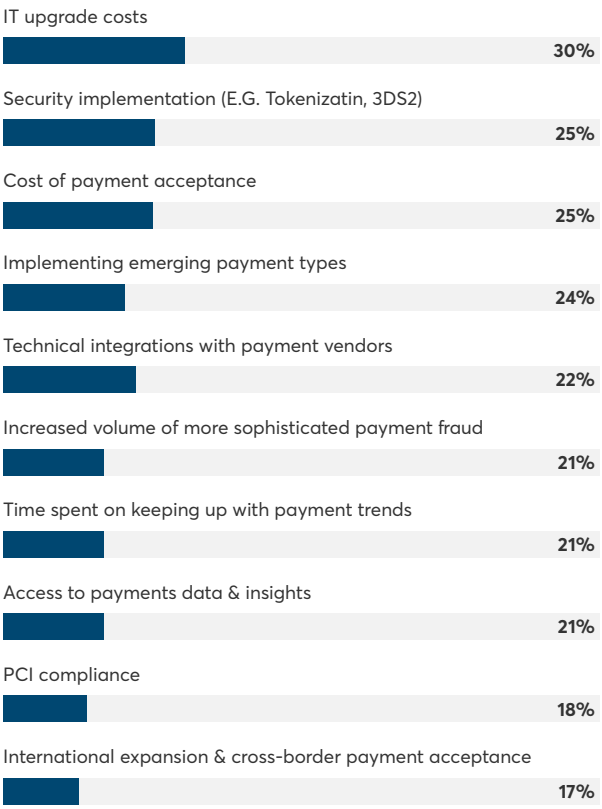


Figure 7 - Source: Global Payment Risk Mitigation, FIS and Forrester

How challenging are the following to your business today?

	PAYMENT FRAUD	CUSTOMER DATA SECURITY
Critical challenge	22%	20%
Very challenging	33%	31%
Not challenging	4%	5%

Figure 8 - Source: Global Payment Risk Mitigation, FIS and Forrester

In any case, Fraud Prevention and Customer Data Security were two most challenging factors for most respondents, compared, for example, to the complexity of integrating and managing multiple payment solutions, which was critical for only 18% of respondents. 55% of the interviewed merchants consider the issue of fraud prevention to be particularly burdensome and over 50% responded in the same way regarding the security of customer data.

The negative effects of the COVID-19 pandemic also include fraud against Ecommerce. The increase in online sales, which has occurred in many sectors, although not all of them, as we have already discussed in our article dedicated to the future of retail, has proved to be a fertile ground for cyber criminals. This was also confirmed by the FIS survey: over 80% of respondents said they had suffered an equal or greater number of frauds compared to 2019, and 59% found an increase in fraud on card not present (CNP) payments.
The majority of the respondents also reported an increase in so-called friendly fraud, and 20% found a steady year-on-year increase in disputes.

24 - Global Payment Risk Mitigation, FIS e Forrester

Has your company detected less, more or an equal amount of the following types of payment fraud in 2020 versus 2019?

	SIGNIFICANTLY MORE	SLIGHTLY MORE	SAME	SLIGHTLY LESS	SIGNIFICANTLY LESS
Card-not-present fraud	21%	38%	25%	12%	3%
Synthetic identity fraud	21%	34%	28%	11%	5%
Chargeback fraud	20%	35%	30%	11%	3%
Card testing	20%	33%	32%	12%	3%
Identity theft/new account fraud	20%	32%	30%	13%	5%
Friendly fraud	22%	29%	31%	13%	5%
Account takeover fraud	20%	30%	31%	13%	5%

Figure 9 - Source: Global Payment Risk Mitigation, FIS and Forrester

Figure 9 highlights the main types of fraud suffered by the companies that participated in the survey. Card-not-present transaction fraud, such as Ecommerce and MOTO (Mail/Telephone order), and Synthetic Identity Fraud are the scams that have increased most significantly.

Analyzing the data by a geographic area, there is a greater frequency of card-not-present payment scams in Europe (59%) and North America (67%) and the synthetic identity fraud is more common in the Asia-Pacific area (61%). In South America the greatest increase was recorded in card-not-present payments, chargebacks and card testing transactions, when a micro-purchase is made to test the validity of a card, typically cloned or stolen. These activities have had a direct and significant impact on many business areas. 60% of respondents said they had suffered economic and productivity losses, 58% had a direct impact on customer churn, back office costs and chargebacks. Over 50% specified other relevant consequences, such as the increase in costs related to lawsuits and the reputational sphere, as well as the increase in transfers and costs for mediation and sanctions. Economic losses due to online fraud in some cases reach considerable amount: 4% of the respondents declared that they had lost even more than 11% of their turnover in 2020 alone. 34% claimed to have suffered losses between 6% and 10% of turnover, 51% lost between 1% and 5% and only 11% said they did not suffer any losses.

What risk management strategies does your company use to mitigate card payment fraud?

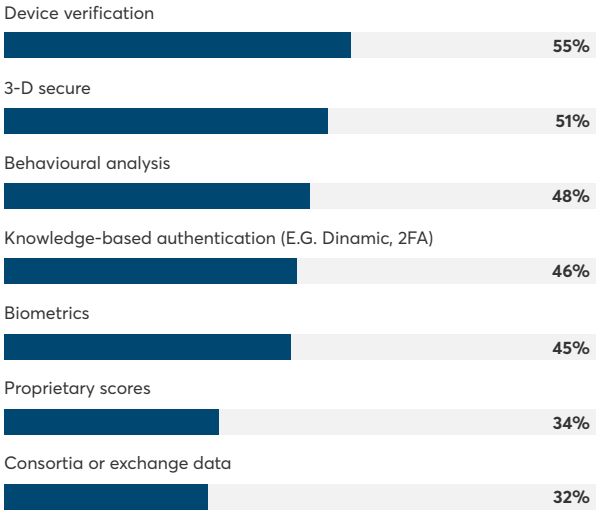


Figure 10 - Source: Global Payment Risk Mitigation, FIS and Forrester

Naturally, all the companies involved have been addressing the issue for a while and have already adopted various solutions, singular or in combination with each other. 55% use the device verification from which the purchase is made, 51% manage the 3DS protocols (it is important to consider that the research refers to 2020, a year

% Distribution of Fraud Losses by Domestic / International Transactions

	2019		2020	
	DOMESTIC TRX	INTERNATIONAL TRX	DOMESTIC TRX	INTERNATIONAL TRX
	DIGITAL GOODS			
SMEs	85%	15%	73%	27%
Mid/Large	86%	14%	78%	22%
	PHYSICAL GOODS			
Mid/Large	74%	26%	69%	31%

Table 2 - Source: 2020 True Cost of Fraud™ Study E-commerce/Retail Report, LexisNexis

before the implementation of PSD2 and SCA), and 48% apply behavioural analysis.
In addition to the main prevention techniques, the following strategies are mitigated: knowledge-based authentication (e.g. 2FA), biometrics, proprietary scores and solutions based on the data exchange.

The use of technologies based on artificial intelligence and machine learning is considered a very important strategic factor by 72% of the managers interviewed, a figure exceeded only by: two-factor authentication, multi-channel analysis (web, app, etc.) and predictive analysis, all these are considered important by 74% of respondents.
The analysis by region of origin of the companies that participated in the survey highlights some peculiarities. C-level and Asia Pacific (APAC) managers stressed the importance of an easy-to-integrate technology stack, real-time insights and two-factor authentication as the most useful tools for fraud detection.

For 73% of European merchants, the key factors are: the applicability of multichannel solutions, two-factor authentication (71% of responses) and 3D Secure protocols (70% of responses). In North America multichannel solutions also received the majority of responses (76%), followed by two-factor authentication (73%) and actionable real-time insights (73%).
In South America, the most frequent response was related to predictive analytics (84%), same goes for artificial intelligence and machine learning tools, while two-factor authentication was considered strategic by 80% of companies.
LexisNexis®, a US company specializing in data analysis and business technology solutions, conducted a survey involving over 800 US Ecommerce merchants and Retailers.[25] The results indicated an increase of 7.3% in fraud-related costs for US retailers and merchants. In 2019, before the pandemic, every dollar of fraud accrued costs equal to $2.87 in Canada and $3.13 in the United States.
Not only that, but also the average number of successful fraud attempts against medium and large companies increased by 43%-48% in the USA. On the other hand, the monthly fraud attempts prevented by the Ecommerce companies, according to the survey results, decreased by approximately 68%.
Analyzing the responses of medium and large US Ecommerce companies that sell digital goods, the cost of fraud per dollar grew from $3.50 in 2019 to $3.73 in 2020 (+ 6.5%) while in the case of physical goods the increase was 8.7% (from $3.11 to $3.38).

The increase in losses occurred in particular for American Ecommerce that also sell internationally through the mobile channel. As can be seen from table 2, the higher costs are related to domestic transactions but it should be noted that the report shows that many attacks occurred through the use of sophisticated bots, which can deceive systems even by changing the geographical origin of the purchase.

During 12 months before the survey, the US online merchants have mainly suffered Friendly Fraud

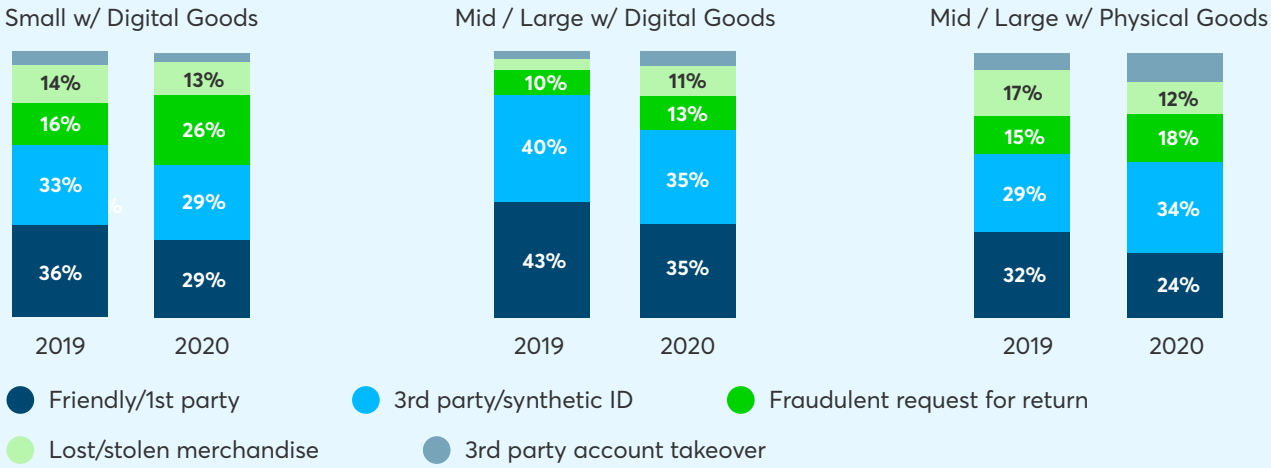
25 - LexisNexis® Risk Solutions 2020 True Cost of Fraud™ Study E-commerce/Retail Report US & Canada Edition July 2020

and Third- Party Fraud, carried out with the use of Synthetic Identity Theft, i.e., false identities that are not attributable to real people but created through the combinations of real data (e.g. social security number) and the invented data (e.g. residence address).

A comparison between 2019 and 2020 highlights the unchanged massive use of techniques related to account takeover or the creation of false identities. Only in the case of small and medium-sized enterprises operating in the field of digital goods, this type of fraud concerns less than a half of cases (48%), while for medium-large companies the data shows rates higher than 60%, regardless of the type of goods sold.
Regarding the distribution of fraud losses by payment method, credit and debit cards present the most consistent data, with 57% of the total.

Compared to 2019, the small-scale US Ecommerce companies witnessed a notable increase in fraudulent card-not-present transactions, which rose from 41% to 55% of total credit card fraud on purchases of digital goods. The losses of purchases with stolen cards have remained constant over time (27%), but have decreased for payments with counterfeit and fake or altered cards, respectively from 15% to 10% and from 14% to 7%.

% Distribution of Losses by Fraud Type 2020 VS 2019



Identity Related Fraud: % Distribution by Activity

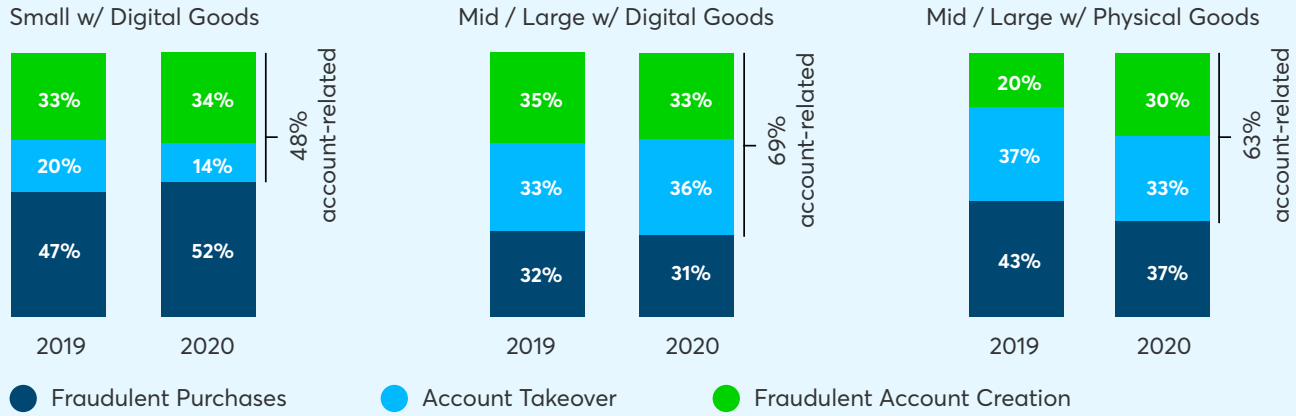


Figure 11 and 12 - Source: Risk Solutions 2020 True Cost of Fraud™ Study E-commerce/Retail Report US & Canada Edition July 2020, LexisNexis®

Even medium and large companies that sell digital goods have witnessed an increase in volumes on card-not-present transactions, from 45% in 2019 to 51% in 2020. The losses deriving from stolen cards have remained constant (23%) and losses from the other categories decreased slightly. For physical goods, on the other hand, the numbers are increasing, albeit not by much. Card-not-present payments in 2020 generated volumes that increased from 43% to 44% while those with stolen cards went from 32% to 33%. On the other hand, the figure attributable to transactions with counterfeit instruments went from 15% to 19% and that with fake cards from 11% to 12%.

Cards are not the only tools with which merchants have undergone illegal activities. In fact, alternative payments, such as PayPal, Bill Me Later and eCheck, to name a few, and basically all the other methods accounted for 20% of the total fraud losses in 2019, are in the list of the most used tools.

Ecommerce fraud in Europe and the United States: the point of view of merchants and consumers

Riskified is an international company, whose mission is to help Ecommerce businesses to realise their full potential by making their Ecommerce safe, accessible and frictionless. The company published a research[26] that involved 4,000 consumers and 400 retailers from the United States, the United Kingdom, France and Germany, where the impact of online fraud was further investigated by comparing the points of view of consumers and of merchants.

The research showed that consumers expect more from merchants in terms of prevention, even to the degree of holding them responsible for the frauds they suffered from. Consequently, they stop buying from the websites, on which fraud has been perpetrated against them. Merchants, therefore, have to counter a phenomenon that generates economic repercussions from many points of view, including the potential sales loss.

> *"It's no surprise that the rapid growth of Ecommerce has also led to a rise in Ecommerce fraud, and as our research shows, the impact is significant for both merchants and consumers."*

Peter Elmgren, Chief Revenue Officer at Riskified[27]

According to the survey conducted by Riskified, 55% of merchants believe they are able to prevent online fraud, but only 34% of consumers surveyed claim they trust Ecommerce businesses' abilities to prevent illegal activities. 26% of the online retailers also say that fraud is significantly damaging their profits, and 34% quantify the loss between 5% and 10% of revenue.

There is, therefore, a disagreement between merchants and buyers regarding the perception of the ability of the online sales sector to prevent fraud. To measure the expectations of the two groups, Riskified created the eConfidence index, where 100 corresponds to the average degree of confidence of the respondents.
As for the merchants, the United States and the United Kingdom reported a higher degree of safety, with a score of 111 and 112 respectively. The responses from German merchants showed a result of 96, while France is the market with the lowest figures among the countries observed – 77 out of 100.
The opinion of the US consumers is similar to that of the US merchants, which is also above average – 107 points. While in the UK consumers' confidence drops to 99. German consumers have a perception of safety on a perfectly average level – 100 points, while the French score falls below average – 94, and the lowest among the 4 countries yet again.

26 - A Crisis of Confidence: Findings from the eCofidence Survey, Riskified
27 - The impact of eCommerce fraud on retailers and shoppers, HELPNETECURITY

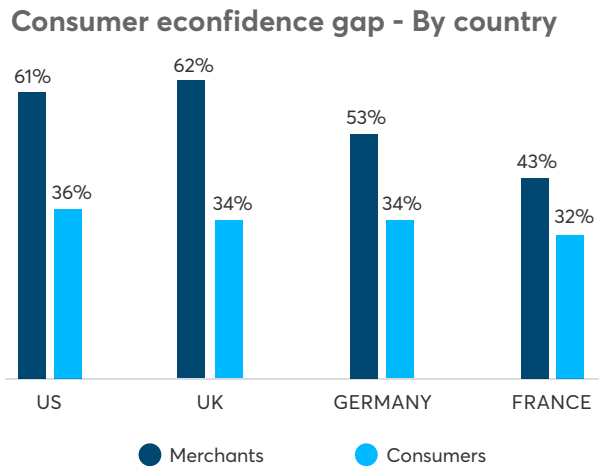


Figure 13 - Source: A Crisis of Confidence: Findings from the eCofidence Survey, Riskified

Riskified's analysis also shows a significant difference in terms of security perception between merchants and acquirers in the United States and the United Kingdom. In France, however, this difference is not as evident, but it still needs to be considered since these same merchants have shown a significantly lower confidence than the rest of the countries involved.

It is also very important to consider that the increase in online sales during the last year and a half has been influenced by the restrictions established by many countries to counter the spread of the pandemic. Therefore, in the near future we might see a rebalancing between online and in-store purchases, even though not at pre-COVID levels, but with a likely downsizing of Ecommerce.

It is of note that among the main reasons why Europeans did not purchase online in 2019, according to Eurostat's data[28], there was a lack of payment security or privacy concerns, as reported by over 20% of the respondents, and this reason is second only to the preference for the in-store shopping experience (almost 80% of respondents). With the continuous increase of digital threats, we have talked about in previous chapters, it is possible that after 2019 the payment security reason has become more relevant.

28 - E-commerce statistics for individuals, Eurostat

PSD2 and Strong Customer Authentication alongside the entire Ecommerce ecosystem

As mentioned before, fraud prevention contributes positively to the entire online payments ecosystem. The European Union is also aware of this, and has introduced the new regulation on payments PSD2 (Payments Service Directive 2), with the objective of increasing competition in the field of payments at a European level and improving the protection of consumer safety, especially in the field of online purchases, helping to strengthen their trust in the whole ecosystem.

The new regulation, whose implementation in Ecommerce started in January 2021, is still in a phase of adjustment throughout Europe. However, the UK is very ahead in terms of transaction authentication, in comparison with most of the EU. The introduction of the Strong Customer Authentication (SCA) concept, i.e. the need for the buyer to authenticate to finalise a payment, has actually increased the security of online payments but, at the same time, has added a further step and friction in the customer journey, affecting negatively the conversion rate and the cart abandonment. Moreover, payments with credit and debit cards, used in most UK Ecommerce shops as demonstrated in figure 14, are not always finalised precisely because of the SCA. Too often, in fact, two-factor authentication of the payment can cause a reduction in the conversion rate, as detailed in our whitepaper "Strong Customer Authentication rate in Europe in 2021".

Share of the top 500 UK online stores with at least one payment method belonging to the following categories

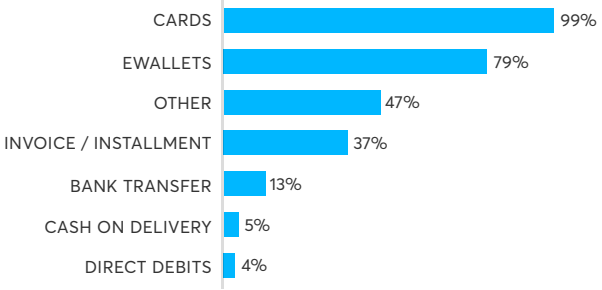


Figure 14 - Source: Statista, Payments Analytics

The whitepaper examines data published by Mastercard that shows the impact of the new European legislation on the shopping carts of all European Ecommerce. The two-factor authentication introduced by PSD2 has the objective of reducing the impact of fraud but, as clearly emerges from the data analysis, it affects the cart conversion rate, effectively devaluing the benefits related to the potential decrease in losses due to illegal activities.

In the end, Strong Customer Authentication is a barrier to entry, which often is not overcome by the buyer. According to what was observed by Mastercard, during the first quarter of 2021, only 74.5% of authentications were successful in Europe, with a very heterogeneous distribution of results. While the United Kingdom is the benchmark for Europe, with 89.5% of authentications carried out correctly, while Italy is positioned closer to the bottom with a result that slightly exceeds 60%, surpassing only Belgium, which registered only 56% of SCA as successfully passed.
Not only that, Italy's performance in frictionless authentication, which has grown mostly thanks to the ability of 7 issuers to leverage exemptions, has led to the least satisfactory result: 12.7% against a European average of 29.6%. This data is particularly significant especially if we consider the results of countries such as Spain, a nation that despite being among the last to adopt the 2.0 flow, registered 38.6% of successful frictionless authentications as of April 2020.
Although the new PSD2 regulation aims to increase competition in the field of payments at a European and UK level, improving consumer safety protection, especially for online purchases, and offering them new opportunities in the field of financial services, there is a clear need on the part of all the stakeholders involved to optimise their implementation in the payment processes.
Therefore, it is necessary for issuers to introduce solutions capable of improving the user experience of consumers during authentication process and for merchants to contribute by improving the process of analyzing the risk of payments and maintaining a high level of security without affecting conversions.
The adoption of effective solutions not only in terms of prevention but also in the identification of false positives, i.e. those genuine payments that could be mistaken for fraudulent by poorly performing prevention systems, could be the keystone for both merchants and for their customers.

Risk analysis and artificial intelligence: Axerve's response to fraud

Artificial intelligence and machine learning are tools that can actively contribute to countering the increasingly sophisticated threats described in previous chapters. 27% of medium/large companies operating in the digital goods sector that participated in the LexisNexis®25 survey said they had integrated these tools, as well as 6% of the companies from the same sector that sell physical products.
However, fraud prevention solutions implementation risks affecting the customer experience, therefore, a complete integration is required that is also able to minimise the frictions during the payment phase. Only 34% of merchants believe they have reached an optimal balance in this area, 48% consider themselves moderately satisfied, and 16% say they are dissatisfied or unable to answer with certainty.

Axerve Guaranteed Payments: artificial intelligence at the service of fraud prevention

Starting from these premises, Axerve has introduced in its offer a fraud prevention solution based on artificial intelligence and machine learning that is fully integrated with the online gateway. Friction reduction in the payment process, decrease of chargebacks and increase of the conversion rate are just a few of the points of strengths Axerve's platform.
The transaction processing involves a series of steps of analysis of the risk of the transaction with an extreme precision, not only through collecting data directly from the merchant, but also enriches purchase orders thanks to a series of tools.

Axerve Guaranteed Payment gathers order details from the merchant.

The platform enrich the data from internal and external sources.

Each order is linked to all the other orders in the database.

Machine-learning models review transactions and return a decision in a fraction of a second.

Orders are evaluated and then approved, declined, prompted for additional information or offered alternate payment.

We review transactions for accuracy and look at larger trends to spot anomalies.

Merchants submit selected details of the orders for evaluation, such as contact information, shipping and billing details. Axerve Guaranteed Payment integrates this information by enriching it through external sources that can provide the e-mail activation date and the buyer's social media profiles.
After external data is collected, the internal data processed by the platform is added to it. The platform uses a beacon that tracks information about the buyers from all the websites that use the same fraud prevention service, including the type of device, the online user behavior and the use of proxies.
The platform is constantly being improved by specialised analysts who contribute to the evolution of the models. In the end, Axerve Guaranteed Payment is able to increase cart conversion and, at the same time, guarantee full refund of any unidentified fraud.

Axerve Advice: how to improve the conversion rate on authentications

Axerve's 3DS2 exemption solution offers merchants the ability to process transactions directly, shifting the liability to the merchant. By integrating the Axerve Guaranteed Payment fraud prevention service, any unrecognised fraud would be 100% supported by Axerve.

The TRA (Transaction Risk Analysis) consists in the real-time assessment of the transaction risk and allows the possible SCA exemption of less than 500 euros. Transactions with low levels of fraud risk can be processed without authentication. Processing them with an exemption request, the probability of the authorisation increases but the responsibility for any fraud remains on the merchant.

Thanks to the Axerve's solution, described in detail in the whitepaper dedicated to the correlation between SCA and conversion rate, the processed transactions are subjected to some checks and, if this phase is passed, they are sent directly into the authorization stage, avoiding a 2-factor authentication. When processing payments, the following checks are made:

- the transaction value must be within the expected threshold, dependent on the acquirer;
- if the risk of the transaction is low, the exemption request is sent, if not approved, it is necessary to proceed with authentication.

The Axerve Advice solution aims to intervene in risk analysis, improving its effectiveness and contributing to an increase in the potential number of transactions finalised without 3DS, which, naturally, can affect conversions.

Axerve Advice (TRA)

Axerve Advice performs a real time risk analysis, allowing for a **TRA exemption** to be requested whenever it is possible.

Authentication

Authorization

Axerve Guaranteed

After the authorization, a second fraud check is performed with Axerve Guaranteed Payments in order **to lift any fraud-related risk** from you.

Ecommerce and the Payment Orchestration revolution

As stated earlier, the constant growth of new Ecommerce customers also has a negative side, namely the increase in online fraud against consumers and companies, despite the increase in initiatives and solutions to counter them.
However, the evolution of payment solutions that overcome digital threats does not depend solely on the innovation of fraud prevention platforms, on the integration of tools compliant with the newly introduced regulations, such as PSD2, or on the greater awareness of buyers, but also on the introduction of tools that manage payments through a sophisticated platform management system and, at the same time, facilitate the coordination of all collections.
Precisely for this the concept of payment orchestration was born, where a single element is able to manage a complex set of collection flows from different sources and payment methods, just like a maestro would orchestrate different instruments in order to achieve the perfect symphony.

Thanks to payment orchestration platforms, each integration collaborates within the system to enable the most efficient path for a fast and secure transaction. This simplifies the process, allowing the merchant to save on additional integrations, while providing a frictionless checkout experience for customers.
Increased conversion rate, scalability, automatic reconciliation, effective fraud prevention, especially in a multi-acquirer context, are just some of the advantages of these platforms. Thanks to the payment orchestration, in fact, it is possible to manage individual payments by connecting them to different PSPs, acquirers and fraud prevention platforms, according to the needs of the merchant.

An evidence for the potential of this approach is the possibility of connecting specific payments to different acquirers to better manage the exemptions allowed by the European PSD2 regulation, as detailed in our article on SCA and 3DS2. In fact, the new European regulation on payments allows the so-called low-value transactions to be exempted from SCA. What qualifies for a low-value transaction, however, may vary depending on the average fraud rate of the acquirer managing the payment.

Thanks to the introduction of default rules, or in more advanced cases, through artificial intelligence, the payment orchestration can direct payments to the ideal acquirer for that specific transaction or to a specific fraud prevention platform, not necessarily offered by PSPs a merchant usually relies on.
In addition, the same approach can be adopted to set up redirections related to the pricing applied by the service provider. Therefore, payments can be sorted by a single market (e.g. American cards to US acquirer or PSP) or by type of payment method (e.g. corporate cards, consumer, digital wallet, etc.).

Fraud Prevention and Payment Orchestration

Recent research by Global Market Estimates (GME)[29], aimed at identifying the market value of payment orchestration platforms by market type, application and a global vertical sector over the period 2021-2026, has identified a steady growth in demand for these services.
According to GME, by the end of 2026 the market for payment orchestration platforms will reach almost 1.5 billion dollars in revenues thanks to the fact that the demand for tools capable of

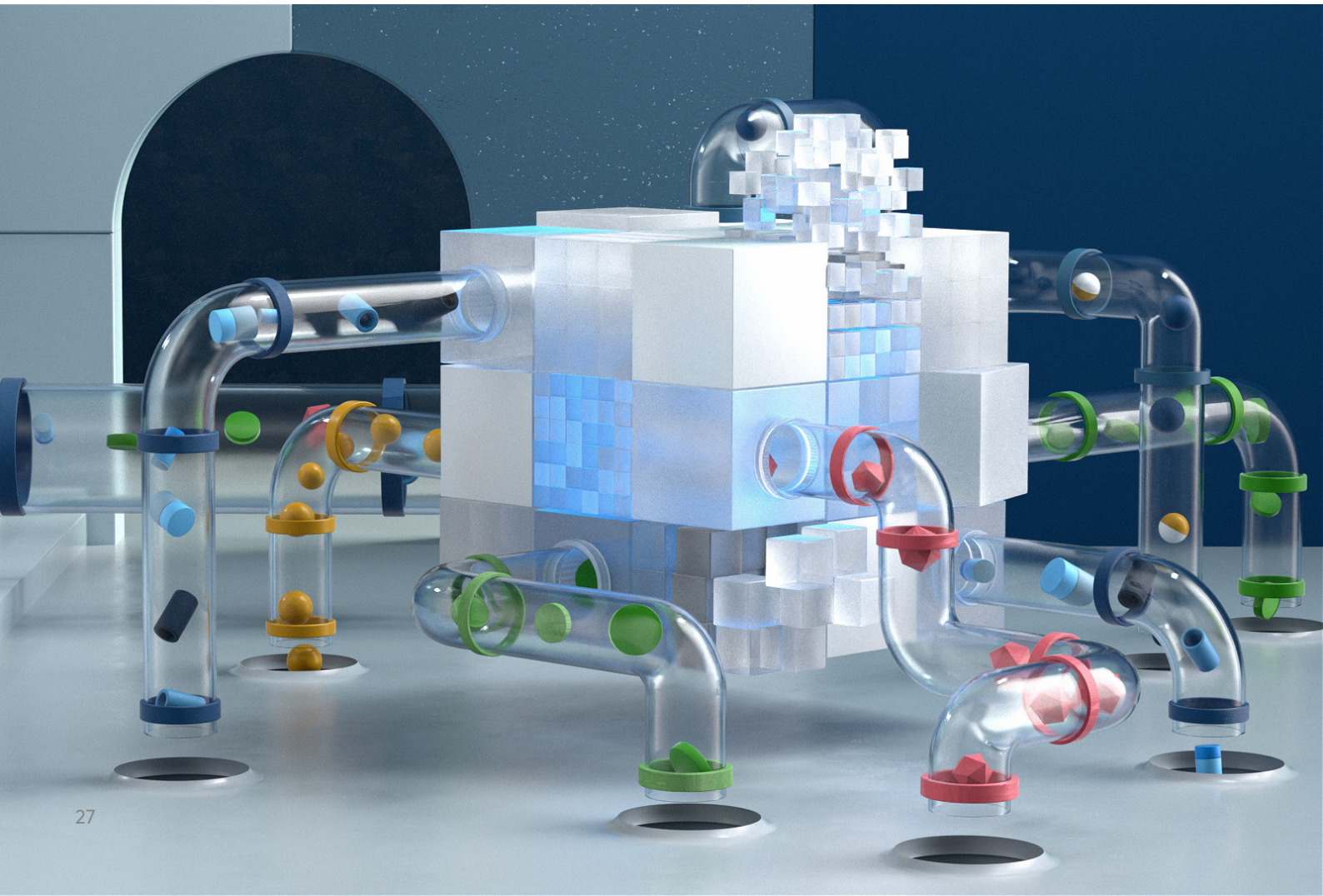
29 - Global payment orchestration market - Forecasts to 2026, Global Market Estimates

managing multiple payment methods will continue to grow, in an increasingly global but regulated context.
In a constantly changing and fragmented scenario, the payment orchestration platforms will fill a void created by the lack of global standards for cross-border payments and providers that are able to provide a uniform and clear view on the collection data, managed by an ever-increasing number of platforms and payment methods.

Among the strengths of these platforms are the collection and analysis of data coming from multiple sources and real-time analytics tools, as well as strategic components for optimizing internally fraud prevention activities. Collecting data from multiple channels takes time and resources and not all solutions offer dashboards that can offer a complete step-by-step view of the transaction's progress.

A homogeneous and complete view of transactions not only makes reconciliation and reporting easier but allows to observe payments more effectively, providing an opportunity to analyse them to contribute to fraud prevention activities, reducing the number of frauds suffered and the number of false positives, increasing the conversion rate of shopping carts.

The opportunities offered by payment orchestration platforms are multiple and in this whitepaper we have only mentioned their advantages in terms of transaction analysis to make fraud prevention more effective. On the Axerve website you can learn more about the potential of the Payment Orchestra™ also by contacting one of our sales representatives, plus in the coming months we will publish new content on the subject in the Learn section.



Sources

1. econsumer.gov Internationa Fraud Report
2. FTC COVID-19 and Stimulus Report
3. New EU cybersecurity strategy and new rules to make physical and digital critics more resilient, European Commission
4. The Internet of Things by 2025, GSMA
5. Crime, Safety and Victims' Rights, European Union Agency for Fundamental Rights
6. Fraud - The facts 2021, UK Finance
7. Digital Trust & Safety Index: Account Takeover Fraud and the Growing Burden on Business, Sift
8. Security Operations Annual Report, Arctic Wolf
9. FRAUD – THE FACTS 2021, UK Finance and LexisNexis
10. GBG Fraud Survey 2020, GBG
11. 2021 MID-YEAR UPDATE CYBER THREAT REPORT, SONICWALL
12. Trend Micro Cloud App Security Threat Report 2020, Trend Micro
13. The State of Email Security Report, mimecast
14. Global Ransomware Damage Costs, Cybersecurity Ventures
15. COVID-19 sparks upward trend in cybercrime, Europol
16. Europol: 10 held for alleged $100m cryptocurrency theft from celebs, others, Reuters
17. The SIM highjackers: how criminals are stealing millions by highjacking phone numbers, Europol
18. Mobile Messaging Adoption Report 2021, Esendex e PricewaterhouseCoopers (PwC)
19. Internet Crime Report 2020, Internet Crime Complaint Center (FBI)
20. Q2 2021 OutseerTM Fraud & Payments Report, Outseer (RSA)
21. 2021 Global Digital Trust Insights, PwC
22. 2021 Gartner Board of Directors Survey, Gartner
23. The global consumer: Changed for good, PwC
24. Global Payment Risk Mitigation, FIS e Forrester
25. LexisNexis® Risk Solutions 2020 True Cost of Fraud™ Study E-commerce/Retail Report US & Canada Edition July 2020
26. A Crisis of Confidence: Findings from the eCofidence Survey, Riskified
27. The impact of eCommerce fraud on retailers and shoppers, HELPNETECURITY
28. E-commerce statistics for individuals, Eurostat
29. Global payment orchestration market - Forecasts to 2026, Global Market Estimates

axerve

Your Payment Partner to Grow

www.axerve.com