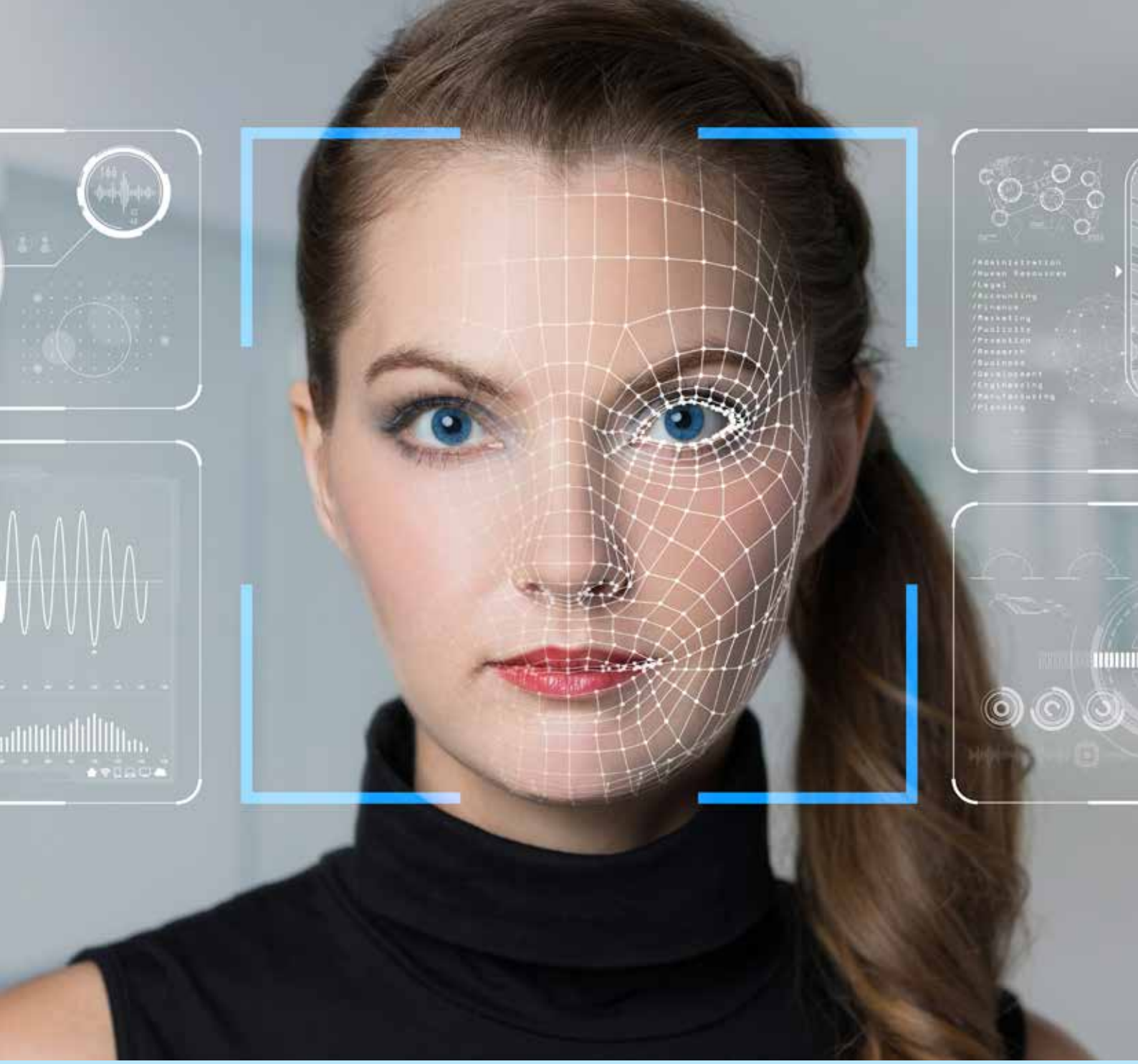


European Fraud Report – Payments Industry Challenges

PAYMENTS INDUSTRY INTELLIGENCE
Payments CARDS & MOBILE

nets

Contents

European Fraud Report 2019

1

Executive Summary

With the total value of fraudulent transactions annually amounting to €1.8 Billion, according to the latest European Central Bank (ECB) report, the need for fraud prevention services has never been greater. We believe that the payment industry needs to tackle the problem of fraud where it starts, in many cases on the Internet and not just where it ends with the customer if we want to ensure trust in our product and services.

It is vital for consumers to continue embracing digital solutions that so many market players in the payment industry are seeking to promote to their customers.

The challenges and threats ahead for the European payment industry are many and this report provides an overview of developments that market players are facing right now.

Among these are the increases across Europe in Card Not Present (CNP) fraud, which now represents almost 80% of the total volume of fraudulent card transactions. Among the factors driving the increases are changes in customer behaviour, but also stronger fraud prevention in other areas, which is forcing fraudsters to seek new sources of illicit income.

Organised crime has caught on to online fraud and are taking advantage of the fact that various types of fraud and scams are readily available for sale on the Internet - also known as Fraud as a Service (Faas) - as are card numbers. This together with the low risk of prosecution makes digital crimes appealing for the criminals.

Data breaches containing Personal Identifiable Information (PII) such as card numbers and new type of skimming being conducted online are just some of the ways that online criminals obtain information that is then sold on the Internet.

While many actors are focusing mainly on communicating to customers about the risk of phishing, we at Nets are equally focusing on CNP fraud and data breaches where they occur on the Internet, as this is one the biggest challenges right now and rarely has anything to do with the customer.

Nordic consumers have been quick to adopt digital solutions and our strong position in the Nordics has allowed us gain valuable insight and knowledge into how to combat fraud in the digitised world.

As the main provider of card fraud prevention solutions in the Nordics, we are proud of the significant lower card fraud ratio in our markets compare to the European average and in the UK and France.

As a service provider in one of the fastest industries, Nets delivers a focus on the customers' needs for feeling safe and secure. We do that by delivering easily adaptable fraud solutions, creating seamless customer experience and supporting any customer journey demand. This combined with bringing together the world's best subjects matter experts and carefully selected future proof counter fraud solutions are at the core of our strategy.

S Gabelgard

Sune Gabelgård
Head of Digital Fraud, Intelligence & Research at Nets Group

www.nets.eu

2

Introduction

We live in a digital payments and post data-breach world. Time and again, technology has pushed the limits of what we thought we could do. It has improved our lives but also poses new challenges: while payment service providers and processing firms learn, improve and innovate, fraudsters also become more creative. Therefore, fraud prevention keeps getting more complex.

The popularity of online shopping and its increased frequency, the proliferation of different forms of digital payments and fewer possibilities for customer verification due to cross-border trade are all things that make fraud prevention more complex.

GDPR, Strong Customer Authentication (SCA) and friendly fraud are other factors that further complicate a fraud specialist's job.

The basics stay the same, but the fraud prevention environment is ever-changing. That means fraud analysts need to be agile, creative and adaptive - just like fraudsters.

Due to changing technologies, digital consumer demands and new fraud trends, legacy systems are often no longer seen as adequate to respond to the latest risk management demands.

GDPR, Strong Customer Authentication (SCA) and friendly fraud are other factors that further complicate a fraud specialist's job.

Fighting fraud can only be done with the right information, though. At this point, no merchant, bank or payment service provider has all the data necessary to determine whether a transaction has been executed by the customer or a fraudster. But the possibility of combining all data across the payments chain on a cross-border level gives us more opportunities to fight fraud.

The key challenge is to exchange this data quickly and safely. We also need to protect the consumer, reducing friction during the purchase process and respecting consumer privacy.
To keep pace with increasing fraud and risk challenges, the industry has tended to outsource technology services and expert capabilities. This means that managed next generation, all-in-one fraud and risk services are in demand from many banks and payment service providers.

This report gives a brief insight into card fraud in European regions, the drivers behind this fraud, and how always-connected consumers and their changing purchasing behaviours are creating fresh challenges for payment service providers and card issuing banks in Europe.

In addition, the report highlights defence mechanisms that European banks can adopt to combat payment fraud. Finally, the report indicates how a managed all-in-one fraud and risk service, combined with next generation dispute management, can be used to cut fraud losses.

In compiling this report we have consulted the results of recurring market research exercises in the European payments industry. In addition, the views of leading banks, payment service providers, payments industry champions and fraud experts have been examined.

3

Payment Fraud in Europe

Card fraud is one of the most fascinating aspects of the payments industry, not least because it is relentlessly changing. EMV implementation and 3D-Secure, combined with Strong Customer Authentication (SCA), have done much to reduce domestic losses from lost and stolen cards in Europe.

However, the war against fraud losses and the changing face of fraud continue to be a threat for the payments industry. Losses from card fraud on the internet and cross-border fraud on domestic cards have grown significantly. Following EMV implementation, card fraud has increasingly moved to countries where POS terminals or online shops have not yet migrated to EMV and SCA, and to cross-border fraud using compromised cards.

The biggest global card fraud challenges are Card-Not-Present fraud (CNP fraud), cross-border fraud and counterfeiting on non-EMV cards. International card fraud continues to be smaller in scale than domestic card abuse but is proportionately far more common – for example, the fraud rate on French cards used abroad in non-SEPA countries was 16 times higher than on domestic transactions. And of course, fraudulent cross-border card transactions continue to grow across all purchase channels.

TOTAL CARD FRAUD LOSSES

The most comprehensive overall measure of card fraud losses is the fraud loss ratio, which expresses fraud losses as a proportion of total card transaction values.

In September 2018, the European Central Bank (ECB) published its 'Fifth Report on Card Fraud' providing insight on a European level. According to the latest ECB report, the total level of card fraud losses amounted to €1.8 billion in 2016.

Card fraud experienced a decline in terms of value of 0.4 percent compared with 2015, and an increase of 35 percent compared with 2012. However, since the value of all card transactions grew by 1.8 percent in 2016 compared with the previous year, fraud as a share of the total value of transactions decreased from 0.042 percent in 2015 to 0.041 percent in 2016.

Compared with 2015, CNP fraud has increased in proportion, whereas fraud at ATMs and POS terminals has become less prominent. In 2016, 73 percent of the value of all fraud losses on cards issued in SEPA resulted from card-not-present (CNP) payments, i.e. payments via post, telephone or on the internet, 19 percent at POS terminals, and 3 percent at automated teller machines (ATMs). An increase in CNP fraud of 66 percent over a period of five years was the main driver for the 35 percent increase in overall fraud during this period.

Card fraud increased in terms of volume number by 27.2 percent over 2015, and by 92 percent compared to 2012. By comparison, the total number of transactions increased by only 9.6 percent in 2016 compared with 2015. Therefore, fraud as a share of the total number of transactions increased to 0.023 percent in 2016, up by 0.003 percent from 2015.

In 2016, the total share of fraud in overall transactions declined slightly for debit cards and increased slightly for delayed debit cards and credit cards compared with the previous year. In total, the share of delayed debit card and credit card fraud in overall transactions remained larger than that of debit card fraud.

COMPARING FRAUD LOSSES IN SELECTED EUROPEAN COUNTRIES – OVERVIEW

According to the domestic associations responsible for card fraud reporting, card fraud losses for individual European countries show significant variation, ranging from 0.5 basis points to 7.3 basis points in 2017.

Value of Card Fraud Losses in Europe

	2012	2013	2014	2015	2016	GR 15/16	CAGR 5Y
Total card fraud losses with SEPA acquired worlwide (€bn)	1.330	1.436	*1.656*	1.808	1.800	-0.4%	9.2%
- thereof CNP fraud losses (€bn)	0.794	0.958	1.031	1.292	1.320	2.2%	15.2%
Value of card fraud losses as a share of the value of transactions	0.038%	0.039%	0.038%	0.042%	0.041%	-2.4%	2.6%
- thereof ATM Fraud in%	17%	14%	12%	9%	8%	-11.1%	-15.9%
- thereof CNP Fraud in %	60%	67%	69%	71%	73%	2.8%	5.4%
- thereof POS Fraud in %	23%	19%	19%	20%	19%	-5.0%	-5.3%
Volume of card fraud losses as a share of the number of transactions	0.017%	0.020%	0.020%	0.020%	0.023%	15.0%	7.5%
- thereof ATM Fraud in%	11%	9%	7%	5%	3%	-40.0%	-22.9%
- thereof CNP Fraud in %	63%	71%	75%	76%	77%	1.3%	7.8%
- thereof POS Fraud in %	26%	20%	18%	19%	20%	5.3%	-11.1%

Source: ECB Fifth Report on Card Fraud: all reporting card payment schemes (CPSs).

Note: The total number of cases of card fraud using cards issued in SEPA amounted to 17.3 million in 2016. The total number of card transactions using cards issued in SEPA amounted to 74.9 billion in 2016.

Regarding the national figures in this report, the losses in 2017 ranged from as low as 0.6 basis points (0.6 bp) in the Netherlands, Denmark (1.3 bp), Norway (1.6 bp) and Sweden (2.1 bp) to 5.3 basis points in France and to 5.0 basis points in the UK.

The Netherlands and the Nordic countries are examples of fraud control best practices in Europe thanks to the managed fraud and risk prevention services of their pan-European processors which cover cross-border fraud prevention expertise.

In contrast, the UK and France continued to experience higher card fraud losses, mainly from CNP fraud on internet purchases, lost and stolen card fraud, and cross-border fraud losses on domestic cards used abroad.

The implementation of EMV cards and 3D-Secure, combined with SCA and emerging tokenisation security, has undoubtedly contributed to declining card fraud losses in Europe.

Following EMV implementation, card fraud has moved increasingly to countries where POS terminals have not yet fully migrated to EMV. This fraud migration has included fraud types such as CNP fraud, ID fraud, cross-border fraud and others.

Another significant reason for keeping card fraud losses at current levels are improved in-house fraud & risk management activities by individual card issuing banks and payment service providers. These companies also benefit from the support of pan-European processors which combine the latest fraud prevention tools with comprehensive fraud and risk prevention services managing fraud cases cross-borders throughout Europe.

Comparative Overview in 2017

	EU (2016)	France	UK	Netherlands	Denmark	Norway	Sweden
Population (m)	512.5	67.1	*66.0*	17.1	5.8	5.3	10.1
Number of cards (m)	812.4	86.0	180.2	32.3	9.0	16.1	20.3
Card payments value (€bn)	3,053.5	527.8	1,143.2	133.9	88.8	88.2	107.6
ATM withdrawals value (€bn)	1,585.0	147.1	238.3	57.8	11.3	9.6	15.0
Total of card fraud losses (€m)	1,800.0	360.7	690.7	11.7	13.3	15.6	25.9
Card fraud loss ratio	0.041%	0.053%	0.050%	0.006%	0.013%	0.016%	0.021%
Issuer fraud losses by channel (ECB)							
- ATM fraud (in%)	8%	12%	3%	12%	13%	7%	11%
- CNP fraud (in%)	73%	73%	77%	74%	72%	81%	70%
- POS fraud (in%)	19%	15%	20%	14%	15%	12%	19%
Sources:	ECB	OSMP	FFA UK	Betaal Vereiniging	Nets	Finanstylsinet	Nets

Notes: Number of cards covers both debit and credit. Card fraud losses cover transactions made domestic and abroad on domestic cards.

Source: ECB, domestic associations, PCM research.

Insights by country

For obvious reasons, the level of card fraud losses can only be seen in the specific context of card use in each country. In particular, the Nordic countries constitute the most advanced and digital-ready payment markets in Europe, and are among the most advanced in the world.

Card fraud losses show different patterns in each country, depending on the specific impact of domestic payment schemes and the digital identity systems implemented to protect, for example, consumers and online purchases.

From a European perspective, dedicated fraud and risk prevention services are practiced by all payment service providers. However, if data on a European level was available, fraud and risk prevention services would benefit and could cut total fraud costs.

In this chapter, the report provides high-level insight for six selected European countries. In most countries, CNP fraud has increased in proportion, whereas fraud at ATMs and POS terminals has become less prominent.

France

The domestic card scheme Cartes Bancaires (CB) is unique to France, with more than 10 percent of CB card payments made on the internet. Indeed, France continues to enjoy the benefits of early adoption of Chip and PIN. However, their local fraud threat has become proficient at the techniques required to compromise credentials. According to fraud experts, France shows early signs of fraud growth in the cyber-enabled space, i.e. criminals are shifting their attention away from CNP Fraud. At the same time, French banks are now pushing consumers to mobile apps, which are often more secure than web-based payment applications.

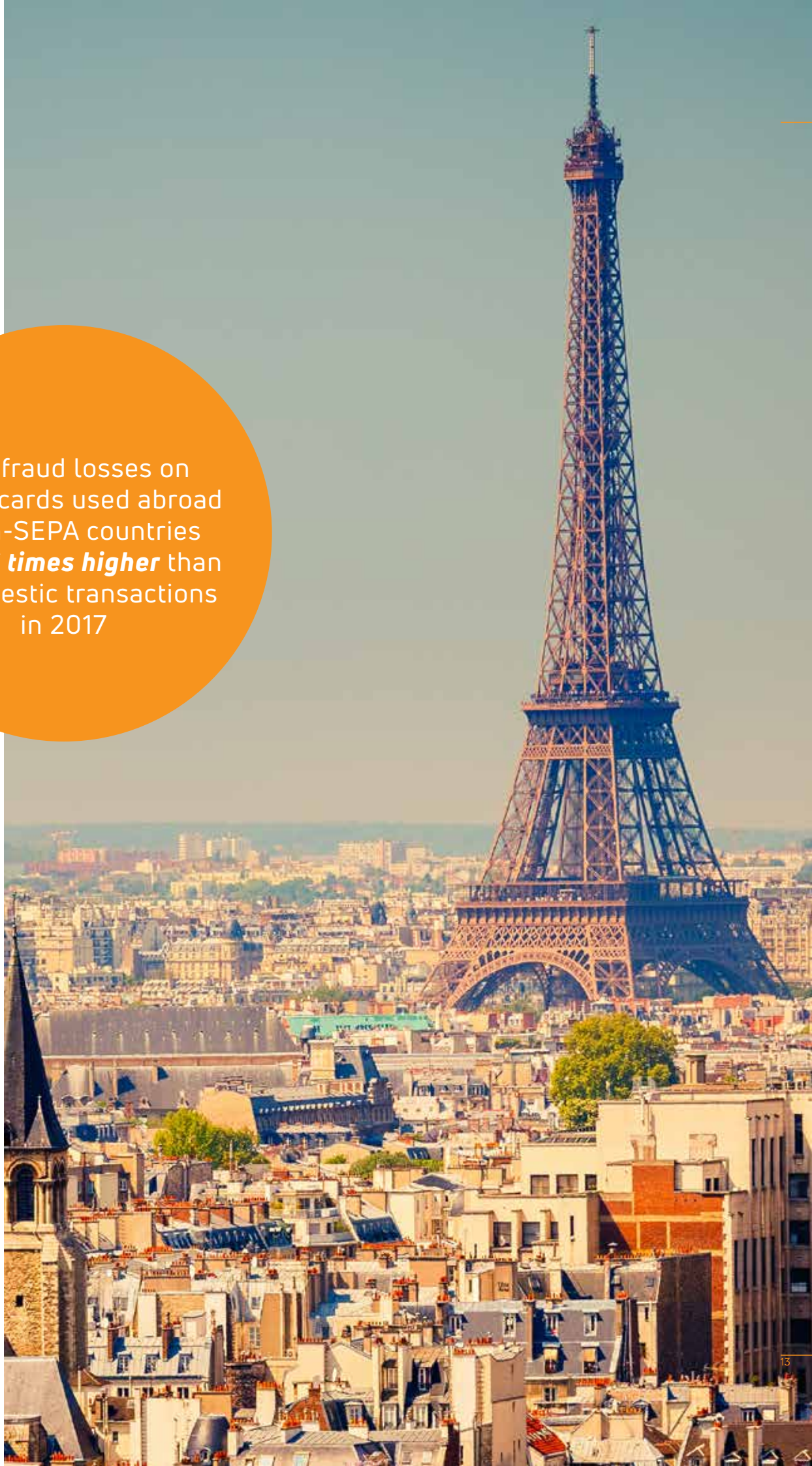
In 2017, card fraud losses were falling, but ID Fraud and stolen cards dominated. In contrast to previous years, the improving position within the French market is the result of reductions in both ID Fraud and Lost and stolen card fraud.

According to the French Observatory for the Security of Payment Means (OSMP), figures for 2017 showed total fraud losses on French cards in France, on French cards abroad and on foreign cards acquired in France, of €467.0 million, down by 9.8 percent from €517.5 million in 2016. By channel, card fraud losses were composed of: ATM fraud (12 percent), POS fraud (15 percent) and a high level of CNP fraud (73 percent).

Domestic fraud losses on French cards have stabilised at 0.032 percent. Fraud on French cards used abroad and on foreign cards in France is much higher. While the loss rate on foreign cards acquired in France has been broadly stable during recent years at just under 30 bp, 2011 saw it rise to more than 89 bp: however, losses in this category declined to 38.6 bp in 2017.

The loss rate on French cards used in the SEPA region has risen sporadically over the past five years to about 30.8 bp in 2017. Card fraud losses on French cards used abroad in non-SEPA countries were 16 times higher than on domestic transactions in 2017 while losses on foreign cards in France were 12.1 times higher.

Card fraud losses on French cards used abroad in non-SEPA countries were ***16 times higher*** than on domestic transactions in 2017



United Kingdom

There is no domestic payment card scheme in the UK. However, the UK has a high use of debit cards and credit cards. Contactless card payments amounted to 34 percent of card payments on UK-issued cards in 2017.

The UK has just reported its highest-ever losses in plastic card fraud since the previous peak in 2008. In 2016, UK card fraud losses increased by 8.8 percent over 2015, which equates to £618 million of losses. However, in 2017, there was a decline by 8.4 percent from 2016. 72.7 percent of this £566 million fraud loss is down to Card Not Present (CNP) fraud. In addition, card lost and stolen fraud (16.3 percent) declined in 2017. By channel, card fraud losses were composed of: ATM fraud (3 percent), POS fraud (20 percent), and a high level of CNP fraud at 77 percent.

The UK is the first market to have significantly reduced CNP fraud in many years as CNP fraud as a whole declined by 5.2 percent compared to2016. Whilst this is a good story for the UK, it should come as a significant warning to other markets for the impending migration of fraud attacks in this category.

E-commerce fraud still accounts for 50 percent of total UK card fraud losses at £310.2 million, as criminals exploit personal and payment details that are retained by an ever-increasingly connected business landscape.

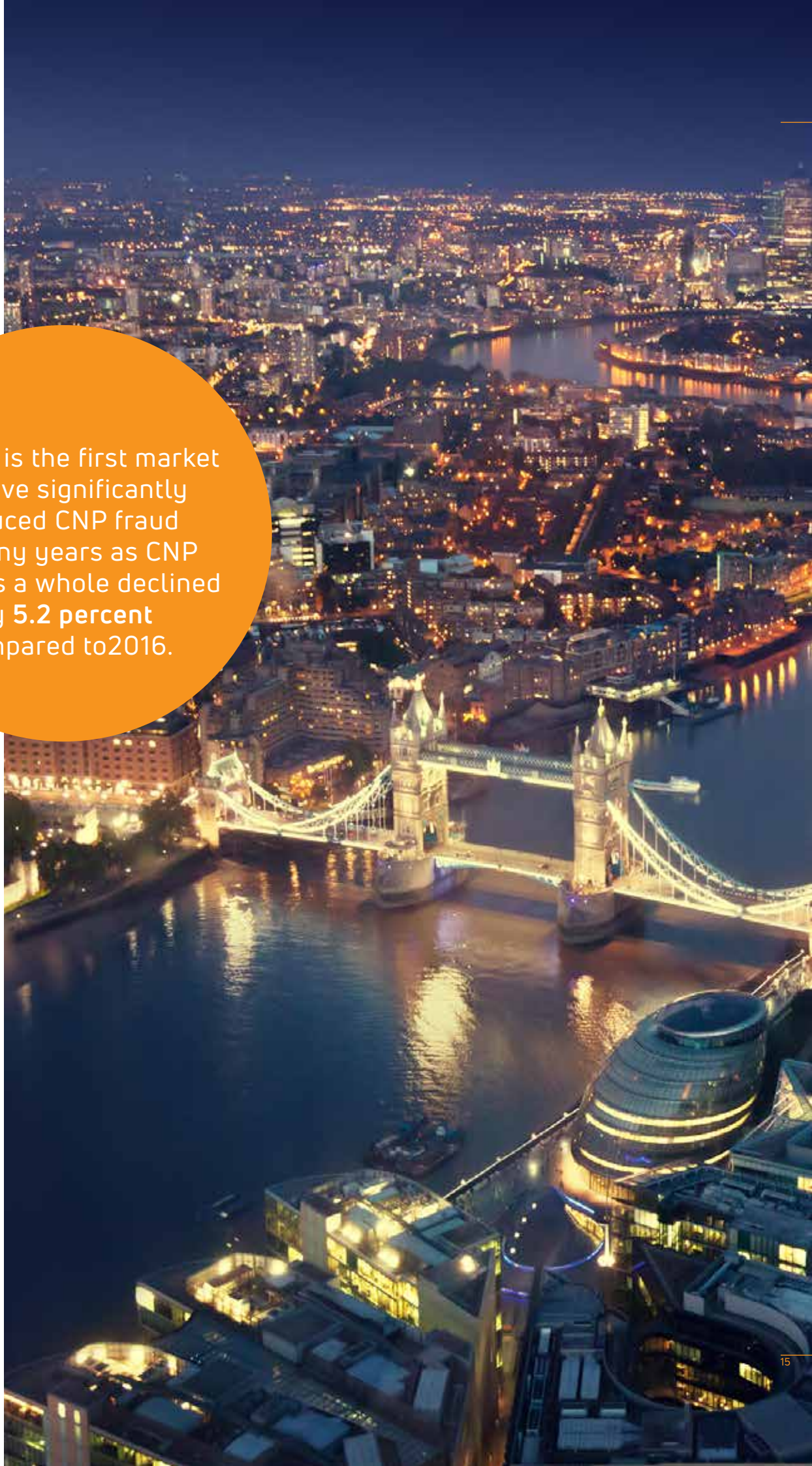
Foreign fraud on UK-issued cards had declined from its 2008 peak to £80.0 million by 2011. Financial Fraud Action UK (FFA, now part of UK Finance) reported that the fraud detection systems used by the banks and card companies to monitor unusual spending were a factor in this decline. However, foreign fraud on UK cards has grown significantly since then, but declined by 20.9 percent in 2017 to reach £158.4 million.

The vast majority of CNP fraud involves the use of card details which have been fraudulently obtained through methods such as skimming, digital attacks including malware and data hacks, or through unsolicited emails or telephone calls. These card credentials are then used to undertake fraudulent purchases on the internet or still by MOTO order.

A second important factor is the high use of credit cards in the UK compared with other European countries. Credit cards can be particularly attractive to fraudsters given the line of credit available. However, UK banks are now pushing consumers to mobile apps, which are often more secure than web-based payment applications.

In May 2019, the UK Payment Systems Regulator (PSR) announced it would consult on giving a specific direction for the implementation of Confirmation of Payee (CoP), with the aim of introducing this new payments security scheme by 31 March 2020. CoP is an important tool to help prevent payment fraud in the UK, as well as accidentally misdirected payments. It works by checking if the name of the account the payment is being sent to matches the name entered.

This initiative will provide customers with better protection from authorised push payment (APP) scams, which cost customers and businesses £354.3 million in 2018 according to UK Finance.



The UK is the first market to have significantly reduced CNP fraud in many years as CNP fraud as a whole declined by **5.2 percent** compared to2016.

Netherlands

As in the UK, there is also no domestic card scheme in the Netherlands. However, all Dutch banks support the domestic online credit transfer service, iDEAL, and most of them the mobile payment app, Payconiq.

Interestingly, the incremental shift from card-based online payments towards credit transfer payments directly from bank accounts has lowered the total fraud rate for payments.

In 2016, the Netherlands implemented a new Dutch digital ID service, iDIN, which is compliant with eIDAS and GDPR regulations. iDIN is a collaboration between the Dutch banks to increase online security.

Dutch banks have been remarkably successful at combating fraud in cashless payments with a fraud rate of only 0.6 basis points, achieving a substantial reduction from its peak in 2012, when card-not-present fraud (CNP) and counterfeit fraud were dominant. CNP fraud is still dominant at 68.2 percent of total card fraud losses, but this is in the context of a 70 percent total card fraud loss reduction since 2008. Around 80 percent of this counterfeit fraud was cross-border.

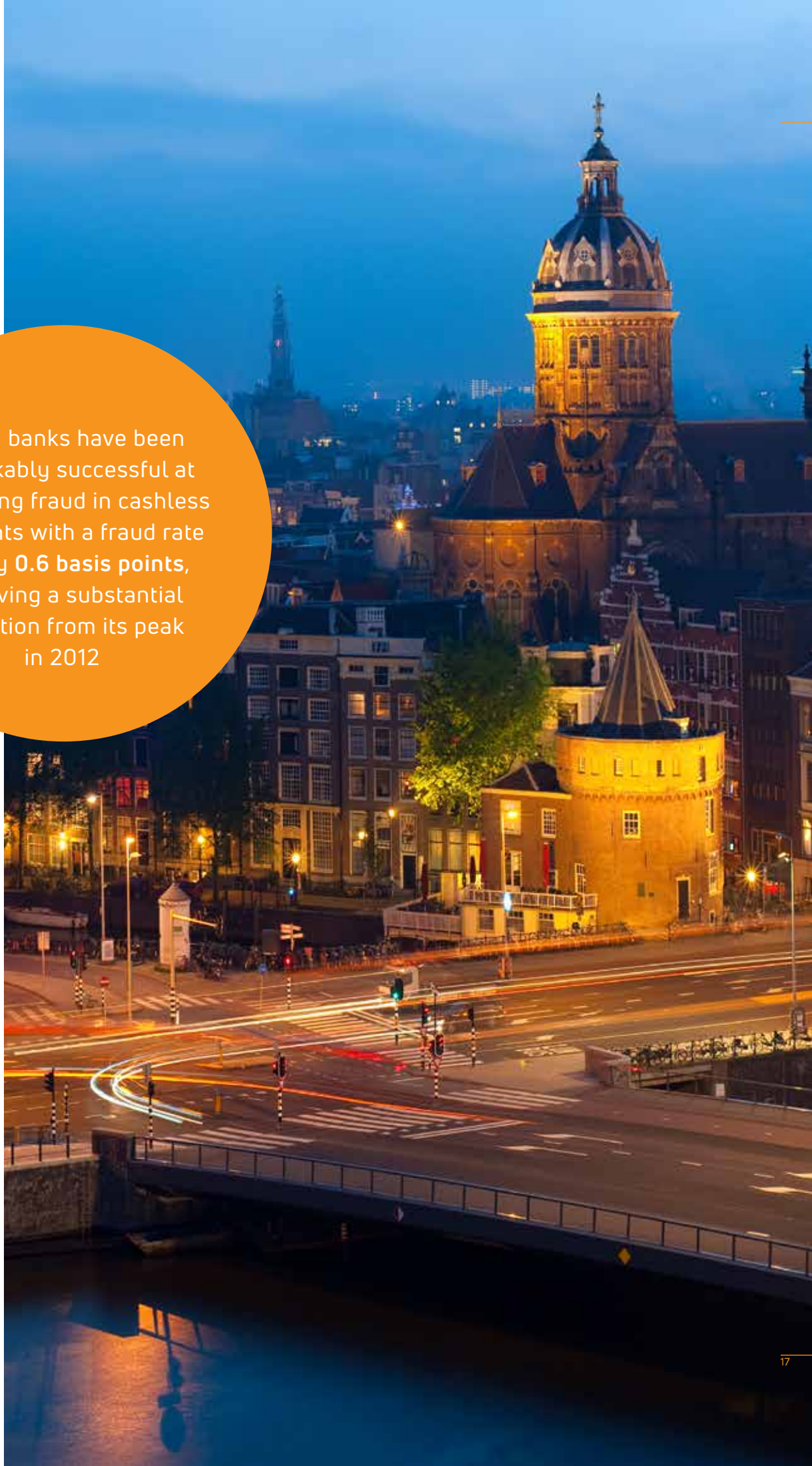
According to Betaalvereniging, the Dutch Payment Association (DPA), total fraud losses in the Dutch payment system were €81.8 million in 2012, and declined to €12.9 million in 2017. However, this figure was up by 26.1 percent over 2016. This is mainly the result of a decline in internet banking fraud and debit card fraud. This figure includes online banking fraud losses, which declined from €34.8 million to €1.2 million in 2017. By channel, fraud in the Netherlands was composed of: ATM fraud (12 percent), POS fraud (14 percent) and a high level of CNP fraud at 74 percent.

The security of retail payments in the Netherlands is comparatively high for several reasons. The fact that overall card fraud losses remain significantly lower in the Netherlands than in comparable European countries suggests that its strategy of online-to-issuer authorisation combined with 3D-Secure, the geo-blocking of debit cards and the use of sophisticated fraud prevention systems by domestic card processors has been effective in combating fraud.

Educational campaigns run by the DPA and the Dutch banks about the types of fraud, as well as coverage in the media, have proven effective. In 2016, the DPA and the banks launched a national campaign to warn the public about debit card dispatch fraud.

The use of credit cards is also a lot lower than debit cards in the Netherlands, and consumers are more commonly using the domestic credit transfer service, iDEAL. With iDEAL, consumers can pay their online or mobile purchases directly from their bank account. This means less card data is out there to be compromised. The Dutch banks are also pushing consumers to mobile apps, which are often more secure than web-based payment applications.

Another best practice for keeping card fraud losses at their current low level is the fraud and risk service support of the domestic card processors across the country.



Dutch banks have been remarkably successful at combating fraud in cashless payments with a fraud rate of only **0.6 basis points**, achieving a substantial reduction from its peak in 2012

Denmark

The domestic card scheme, Dankort, is specific to Denmark. From 2016, all new and renewed Dankort cards have an additional contactless NFC function. Mobile HCE NFC payments are also available with Dankort cards, and Danish consumers can load their Dankort debit card onto NFC capable smartphones and use it to make in-store payments.

In spring 2017, Nets launched the Mobile Dankort app. In April 2017, 64 banks cooperating as BOKIS added Mobile Dankort to their mobile HCE NFC payments wallet, BOKIS. From 2017, Danes have been able to make in-store mobile payments using their Dankort card by tapping their phone against BLE capable POS/MPOS terminals.

Many Danes use a MobilePay app for sending and receiving of money without entering card details or account details. At the same time, Danish banks are also pushing consumers towards mobile apps, which are more secure than web-based payment applications.

The Nordic region continues to see a growth in CNP fraud, mainly due to the move towards a cashless society in many markets. Denmark in particular has continued to see concerted growth in CNP fraud, which is now driving the country's net loss position. CNP losses have doubled in the past three years and show no signs of slowing as fraudulent attacks continue to migrate across Europe, away from France and the UK.

Thus, from a very low level, Denmark has seen an increase of 84.5 percent in card fraud losses since 2012. Due to high card limits on Danish-issued cards, Denmark has an unusually high amount of Lost and Stolen fraud, which accounts for a staggering 52.7 percent of total losses. This has been reduced in 2018 by 50 percent following cooperation between Danish police and Nets.

Another explanation for Lost and Stolen fraud in Denmark is the digitalisation of banking and the closure of many bank branches. Many Danish banks accommodated their customers' demand for cash by providing most Danish cardholders with high card limits for cash withdrawals at ATMs and cash-advances in merchant checkouts.

In 2017, card fraud losses amounted to just €11.3 million. This is equivalent to 1.3 basis points, and an increase of 7.5 percent over 2016. In 2017, CNP fraud constitutes 39.6 percent of total card fraud losses, up 3.9 percent over 2016. This compares with 24.7 percent in 2011. By channel, card fraud losses were composed of: ATM fraud (13 percent), POS fraud (15 percent), and CNP fraud (72 percent).

DANKORT FRAUD

For Dankort and international payment cards, most fraud takes place on the Internet. Since 2007 there has been more payment card fraud on the internet than in retail outlets. According to Nets, in 2017, it was 0.019 percent. Dankort card fraud losses totalled DKK 97.7 million. Fraud in connection with CNP sales, primarily via the Internet, again constituted close to 50 percent of all fraudulent use. Fraudulent use of the Dankort continued to be low in an international comparison.

In 2018, Nets has succeeded in creating a seamless 3D-Secure solution for Dankort cards. Danish merchants have reported that they experienced zero abandonment rate and no fraud since implementation.

CONTACTLESS FRAUD

According to the Danish central bank, DNB, fraud patterns in Denmark have changed gradually along with the prevalence of contactless payments. Numerically, contactless fraud constitutes a larger share of fraud than contactless's share of total payments. In Q2 2018, contactless card fraud constituted 65 percent of total fraud, while the number of contactless payments constituted 56 percent of the total payments. In terms of value, contactless fraud constitutes a smaller share. The majority of this amount comes from fraud with chip payments.

In Q2 2018, the average fraud with contactless payments amounted to DKK 189, while for chip payments the average fraud amount was DKK 2,194. At first glance, contactless payments have made low-amount fraud easier. However, risk is reduced at higher levels of transaction value as PIN numbers must be entered when the amount is above DKK 350 or after a series of repeated transactions below the contactless limit.

Denmark has an unusually high amount of Lost and Stolen fraud, which accounts for a staggering **52.7 percent** of total losses.

Norway

The domestic card scheme, BankAxept, is specific to Norway. From 2016, all new and renewed BankAxept cards have an added contactless NFC function. In addition, many Norwegians use the Vipps app for person-to-person payments. Norwegian banks are also pushing consumers to mobile apps, which are more secure than web-based payment applications.

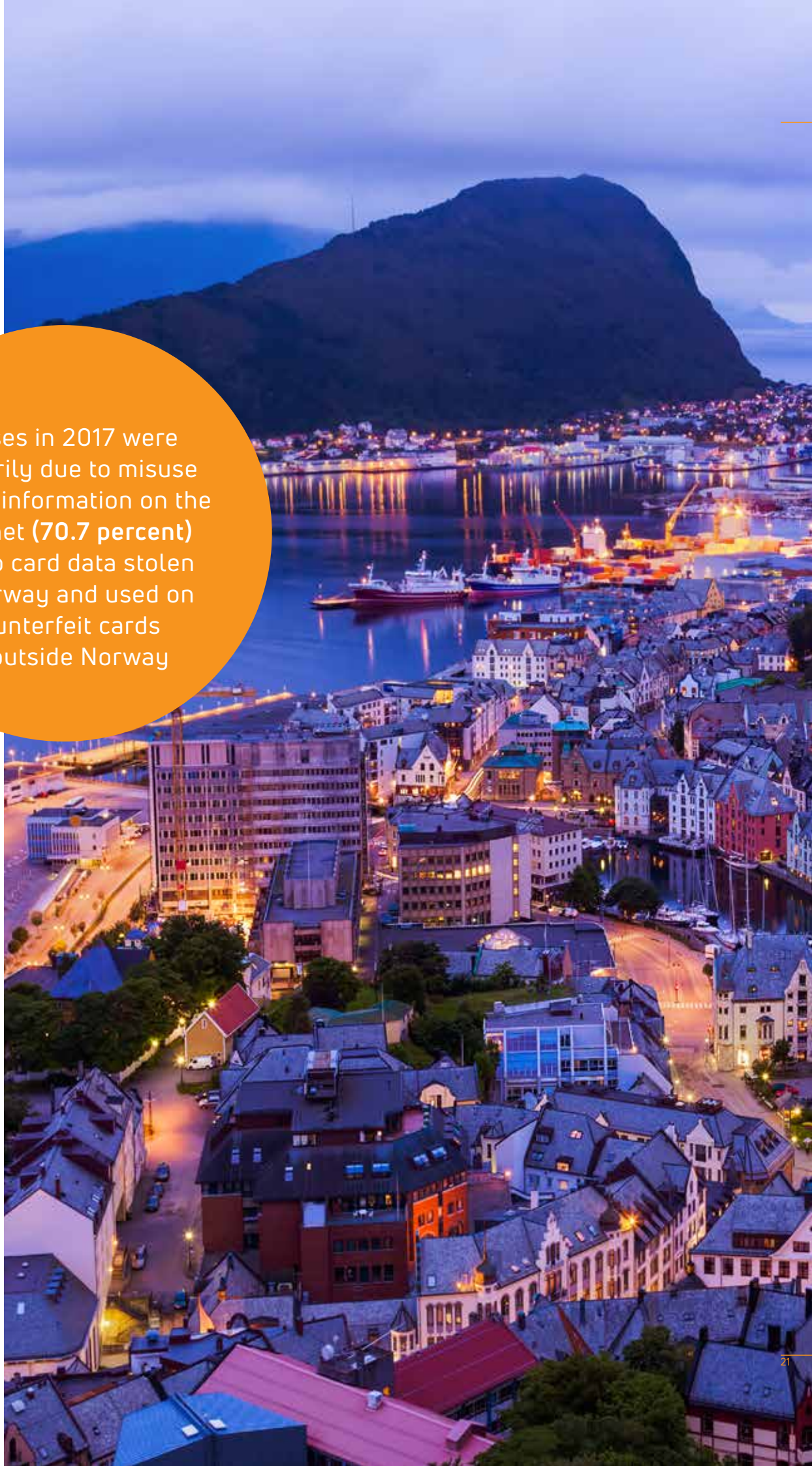
In 2004, Norway implemented a digital online identification and signature service, BankID, now compliant with eIDAS and GDPR regulations. BankID is a collaboration between Norwegian banks to increase online security for consumers. BankID is an important element of the Norwegian payment system and helps banks to maintain a high level of security. It is also used by consumers for online purchases.

The Nordic region has been experiencing a large increase in CNP fraud and Norway is no exception, with a steady growth of that loss line as fraudulent attacks continue to migrate across Europe. According to the national central bank, Norges Bank, fraud amounted to 0.016 percent (1.6 basis points) of the total volume of card payments in Norway. However, if online shopping with cards issued in Norway is considered (NOK 109.9 billion in 2017), card fraud losses would be reduced to 0.132 percent.

In 2017, the Norwegian banks recorded NOK 145.6 million in losses connected with misuse of payment cards, up from NOK 126.0 million in 2011, and equivalent to NOK 176.9 per million of card payments value.

Losses in 2017 were primarily due to misuse of card information on the internet (70.7 percent) and to card data stolen in Norway and used on counterfeit cards in/outside Norway (12.3 percent). Many of these losses are also due to lost or stolen cards (17.0 percent) that are misused with PIN codes in Norway.

Credit card fraud prevention measures taken have been: pushing 3D-Secure combined with risk-based authentication (RBA), updating banks' fraud prevention systems and real-time-scoring, implementing more rule-based fraud control mechanisms. Also, issuers offer PIN selection at ATMs and SMS notification to inform cardholders about the use of their credit card.



Losses in 2017 were primarily due to misuse of card information on the internet **(70.7 percent)** and to card data stolen in Norway and used on counterfeit cards in/outside Norway

Sweden

There is no domestic debit card scheme in Sweden. However, the immediate payment service, Swish, is unique to Sweden. Launched in 2012, Swish includes a mobile payment app which enables private individuals to send money to other users in real time by connecting mobile phone numbers to bank accounts. Swedish banks are also pushing consumers to mobile apps, which are often more secure than web-based payment applications.

The Swedish payment infrastructure includes BankID electronic identifications issued by the major Swedish banks. The majority of these banks also use BankID for electronic identification and signing at their internet banks. BankID is compliant with eIDAS and GDPR regulations.

The Nordic region has experienced a large increase in CNP fraud and Sweden is no exception, with a steady growth of the loss line as fraudulent attack continues to migrate across Europe.

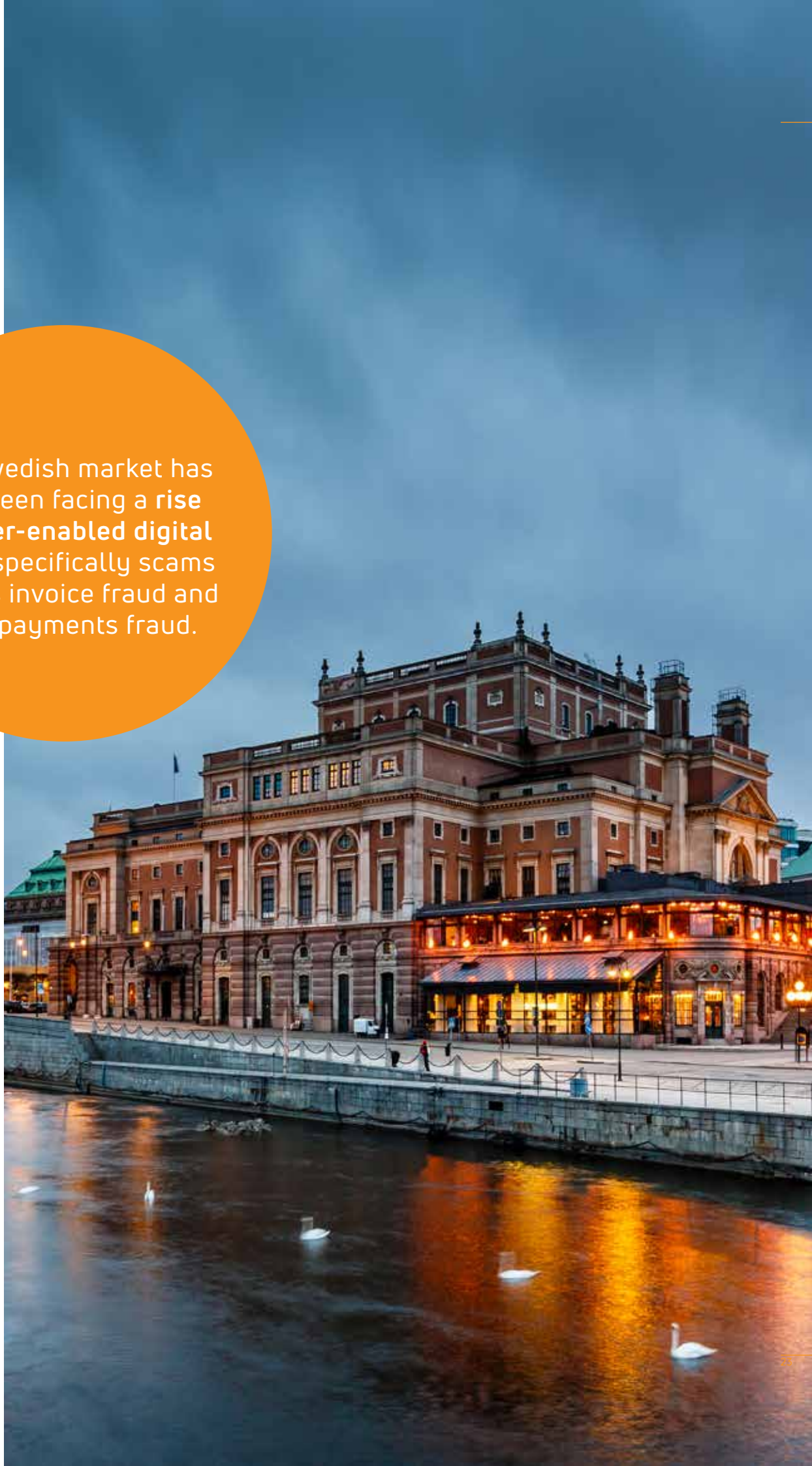
The Swedish market has also been facing a rise in cyber-enabled digital fraud, specifically scams such as invoice fraud and push-payments fraud. In recent weeks, the Swedish regulator took action to confirm that liability for some of these digital scams will shift to banks. This will drastically change the fraud loss landscape of the market and is also likely to influence a liability shift within the region.

Swedish card issuers and banks will need to look at their adoption of enterprise fraud tools and prevention frameworks, in order to combat these threats and ensure control over these ever-escalating loss types.

According to market insight, Sweden has 16.8 percent more card fraud losses than it had in 2012. In 2017, card fraud losses amounted to a low figure of €25.9 million, equivalent to 2.1 basis points, down 0.2 percent from 2016. However, the 25.6 percent share of card lost or stolen fraud is significant, and counterfeit fraud accounted for 21.8 percent of the total card fraud mix. In 2017, CNP fraud made up 48.6 percent of total card fraud losses, up by 0.6 percent on 2016. By channel, card fraud losses were composed of: ATM fraud (11 percent), POS fraud (19 percent), and CNP fraud (70 percent).

Denmark, Norway and Sweden are examples of fraud control best practices in Europe thanks to the support of a pan-Nordic and pan-European processor which combines the latest fraud prevention tools with comprehensive fraud and risk prevention services. This enables these countries to manage fraud cases and fraud data cross-borders at both the Nordic and pan-European levels.

The Swedish market has also been facing a **rise in cyber-enabled digital fraud**, specifically scams such as invoice fraud and push payments fraud.



Method of Compromise

The method of compromise refers to the means by which fraudsters obtain payment cards or card details.

Notable methods of compromise in a complex payment world are CNP fraud based on theft of card credentials and card lost and stolen fraud, followed by growing ID fraud and finally cross-counterfeit fraud.

The main method of compromise responsible for losses in many European countries is now the theft of card credentials. A high proportion of these card fraud losses are caused by the growth in e-commerce, and low use of strong customer authentication methods such as 3D-Secure.

According to a survey carried out by Eurostat, the Statistical Office of the European Community, 77 percent of UK individuals purchased goods or services on the internet in 2016 compared with 59 percent in France, 73 percent in the Netherlands, 66 percent in Denmark, 66 percent in Norway and 66 percent in Sweden. (Eurostat Data: Internet use in 2018: households and individuals). In addition, around 50 percent of online purchases are made with mobile devices.

The report shows a breakdown by method of compromise for France, the UK, the Netherlands and three Nordic countries. They are all reported based on similar categories (see Table N3).
Table N3: Card fraud losses by method of compromise (2017)

FRANCE

The main methods of compromise responsible for fraud losses are lost and stolen fraud (15.6 percent) and CNP fraud (72.5 percent) based on theft of card credentials. Together, the two categories accounted for 88.1 percent of losses in 2017. Theft of card details accounted for 66.1 percent of total domestic card fraud losses in France.

THE UK

The UK shows a similar pattern to France. The main methods of compromise responsible for fraud losses are lost and stolen fraud (16.3 percent) and CNP fraud (72.3 percent) based on theft of card credentials. Together, the two categories accounted for 88.6 percent of losses in 2017.

Other notable fraud categories in France and the UK are counterfeit and ID Fraud (i.e. account takeover/fraudulent card application form).

THE NETHERLANDS

From a very low level of card fraud loss, the main methods of compromise responsible for fraud losses are counterfeit fraud (27.3 percent) and CNP fraud (68.2 percent) based on theft of card credentials. Together, the two categories accounted for 95.5 percent of losses in 2017.

DENMARK

From a very low level of card fraud loss, the main methods of compromise responsible for fraud losses are lost and stolen fraud (52.6 percent) and CNP fraud (39.6 percent) based on theft of card credentials. Together, the two categories accounted for 92.2 percent of losses in 2017.

Card fraud losses by method of compromise (2017)

(in € m)	F	UK	NL	DK	N	S
Counterfeit cards	11.0	41.9	1.8	0.0	1.9	5.6
Card lost or stolen fraud	56.3	112.9	0.0	7.0	2.6	6.6
ID fraud	28.3	36.5	0.3	0.3	0.0	0.0
Card not present fraud	261.6	499.5	4.5	5.3	11.0	12.6
other losses	3.5	0.0	0.0	0.7	0.0	0.5
Value of card fraud losses (in € m)	360.7	690.7	6.6	13.3	15.6	25.9
Counterfeit fraud in%	3.0%	6.1%	27.3%	0.0%	12.3%	21.8%
Card lost or stolen fraud in%	15.6%	16.3%	0.0%	52.6%	17.0%	25.6%
ID fraud in%	7.8%	5.3%	4.5%	2.2%	0.0%	0.0%
CNP fraud in%	72.5%	72.3%	68.2%	39.6%	70.7%	48.6%

Note: figures of non-euro countries were calculated in euro equivalent.

Source: national central bank sources, PCM research.

NORWAY

From a very low level of card fraud loss, the main methods of compromise responsible for fraud losses are counterfeit fraud (12.3 percent), lost and stolen fraud (17.0 percent) and CNP fraud (70.7 percent) based on theft of card credentials. Together, the three categories accounted for 91.1 percent of losses in 2017.

SWEDEN

From a very low level of card fraud loss, the main methods of compromise responsible for fraud losses are counterfeit fraud (21.8 percent), lost and stolen fraud (25.6 percent) and CNP fraud (48.6 percent) based on theft of card credentials. Together, the three categories accounted for 96.0 percent of losses in 2017.

However, simply looking at total fraud losses on the cards of a country by method of compromise hides important regional differences. Such as different method of compromise profiles of card fraud losses in the SEPA region and in non-SEPA country both compared with the domestic card fraud losses. For example, the regional breakdown on French card fraud losses for 2017 illustrates a more complex card fraud loss picture important for fraud prevention measures:

- **Domestic –** The main methods of compromise responsible for domestic fraud losses on French-issued cards are lost and stolen fraud (32.4 percent) and fraudulent use of misappropriated card numbers (65.6 percent) based on theft of card credentials.
- **SEPA region –** The main methods of compromise responsible for fraud losses on French cards in the SEPA region outside of France are lost and stolen fraud (8.5 percent), counterfeit cards (3.8 percent) and the fraudulent use of misappropriated card numbers (85.8 percent) based on theft of card credentials.
- **Non-SEPA region –** The main methods of compromise responsible for international fraud losses on French cards are the fraudulent use of misappropriated card numbers (64.9 percent) based on theft of card credentials, followed by counterfeit cards (13.4 percent) and lost and stolen cards (8.0 percent).

A Geography of Misuse in Europe

The breakdown of card fraud losses by method of compromise shows the importance of distinguishing between domestic and cross-border fraud losses. A clear effect of more stringent anti-fraud measures in domestic markets has been that the fraudulent use of cards has moved from domestic to cross-border, into locations where anti-fraud protection is weaker at present.

From 2012, the value of all payment transactions was marked by an increase in cross-border transactions within SEPA, up by 10.2 percent over 2015, with the share of cross-border fraud within SEPA increasing by 2 percent of total fraud losses.

From a geographical perspective, the ECB provided the following cross-border card fraud insights for the SEPA region:

- Domestic transactions accounted for 90 percent of all transactions, but only 35 percent of total fraud
- Cross-border transactions within SEPA accounted for 8 percent of all transactions, but 43 percent of total fraud
- Although only 2 percent of all transactions were acquired from outside SEPA, they accounted for 22 percent of total fraud

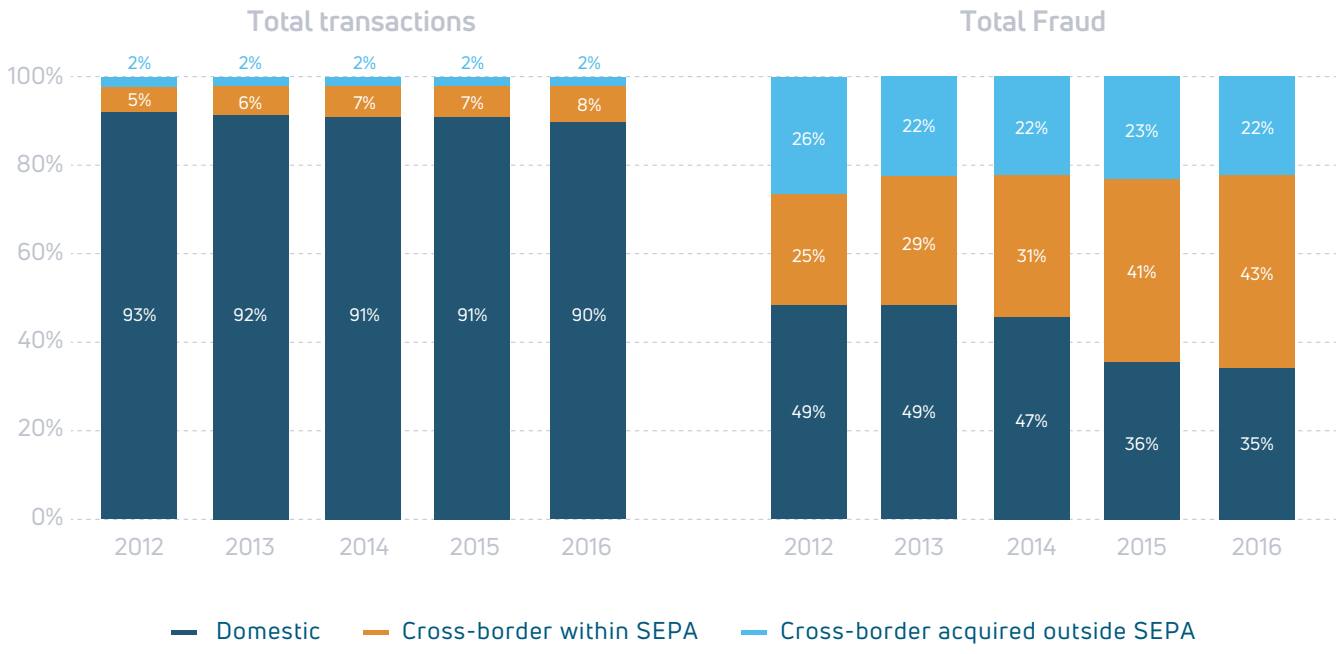
According to market insight, the geographical composition of card fraud largely depends on the type of fraud:

- Lost and stolen card fraud typically takes place at the domestic level, whereas counterfeit card fraud is typically committed outside SEPA
- For counterfeit card fraud, the proportion of fraud committed outside SEPA decreased in 2016 compared with the previous year
- For lost and stolen card fraud, there was a slight drop in the proportion of domestic fraud at the expense of a rise in cross-border fraud acquired inside SEPA

As in previous years, levels of fraud were lower in the euro area than in SEPA as a whole. Data on fraud and transactions using cards issued inside and outside SEPA show that fraud losses incurred outside SEPA on cards issued inside SEPA were lower than losses incurred inside SEPA on cards issued outside SEPA.

In addition, the ECB key findings and market experts suggest that European residents benefit from high European payment security standards and from a high level of security features of their cards, even though the proportion of ATMs and POS terminals outside SEPA making use of enhanced security features is still small.

Evolution of the value of domestic and cross-border fraud (ECB: 2016)



There is evidence of much higher fraud losses on cards used abroad compared to domestic card fraud losses for example in the figures for France and the UK.

FRANCE

In monetary terms, cross-border fraud losses on French-issued cards in the SEPA region and abroad accounted for 27.9 percent and 16.7 percent of total card fraud losses in 2016 respectively. This compares with a cross-border card transactions value of just 6 percent of total card transactions on French cards.

THE UK

cross-border card fraud losses on UK-issued cards accounted for 28.0 percent of total card fraud losses in 2016 compared with the international card transaction value of just 12 percent of the total card transaction value for UK cards.

Foreign fraud on UK-issued cards had declined from a £230,1 million peak in 2008 to £80.0 million in 2011. The FFA cited fraud detection systems used by the banks and card companies to monitor unusual spending as a factor. However, foreign fraud on UK-issued cards has grown again significantly, but with a decline of 20.9 percent to £158.4 million in 2017.

This decline is likely to reflect more pre-notification by cardholders travelling abroad, greater monitoring of international transactions, more transaction declines in locations identified as high-risk and the EMV implementation in non-European regions.

THE NETHERLANDS

Since Dutch banks started using geo-blocking to protect debit cards from fraudulent payments and cash withdrawals outside Europe, cross-border card fraud losses have declined, and losses caused by skimming have stabilised at around €1.5 million (2012: €29 million).

THE NORDIC REGION

With its very low levels of card fraud losses, the Nordic countries are in a comfortable position. Important reasons for the decline in card fraud are the increased use of chips, regional blocking, mobile notification and cooperation with effective police work and law-enforcement.

In addition, the Nordic banks benefit from the support of the fraud and risk management services of the pan-European and Nordic processor, Nets, which combines the latest fraud prevention tools with comprehensive fraud and risk prevention services. These services help Nordic banks and processors to manage fraud cases and fraud data in the Nordic region and across borders at a pan- European level.

Type of Misuse by Category

Looking at the type of misuse, the broadest breakdown is between card payments and cash withdrawals on cards and also by the type of purchase channel, i.e. ATM, POS and internet.

According to the ECB, the combined value of ATM and POS fraud decreased by 5.9 percent in 2016, and the values of both ATM and POS fraud also decreased individually. The decrease in ATM fraud values – down by 12.4 percent in 2016 – was more pronounced than for POS and was driven by considerably lower losses on counterfeit and lost and stolen card fraud in absolute values in 2016 compared with 2015.

At POS terminals, a 21.5 percent decrease in card-not-received fraud losses and a 1.9 percent decrease in counterfeit and lost and stolen card fraud in 2016 contributed to the overall decrease of POS fraud by 3.0 percent.

From 2015, fraud using lost and stolen cards became the most onerous type of ATM fraud, followed by fraud using counterfeit cards. At POS terminals, counterfeit card fraud and fraud using lost and stolen cards were the most prevalent categories in 2016.

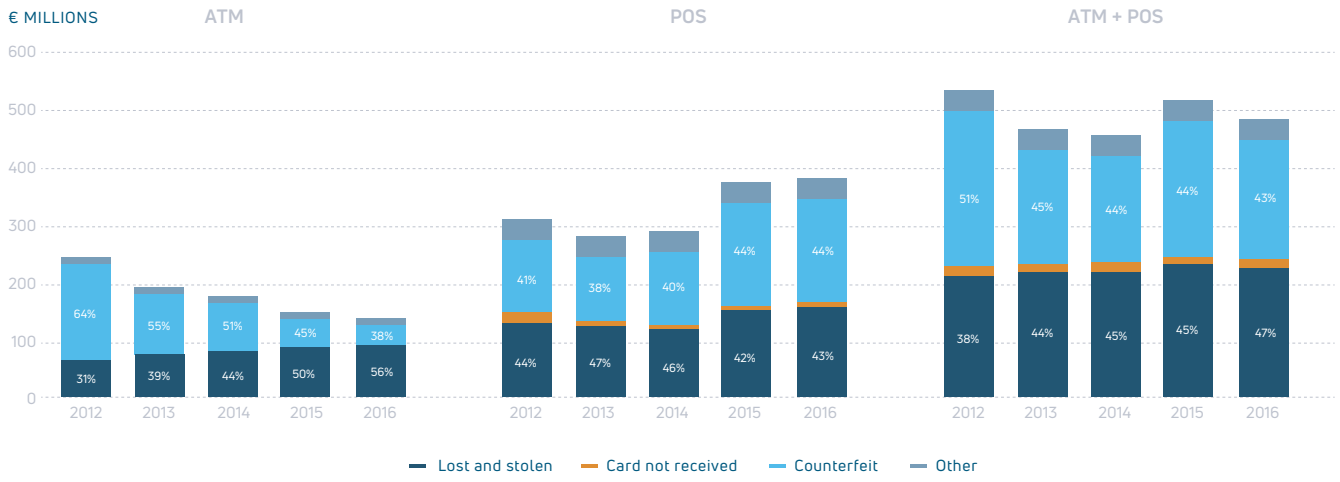
From 2012 to 2016, the value of counterfeit card fraud at ATMs and POS terminals combined decreased by 24.4 percent, while card-not-received fraud decreased by 39.1 percent, albeit from a comparatively low level. Over the same period, lost and stolen card fraud increased by 9.9 percent and became, after 2014, the most prominent category of card-present fraud in absolute value.

CARD-PRESENT FRAUD

decreased substantially between 2012 and 2016, falling by 9.5 percent. EMV migration in Europe reached 84.9 percent in 2016 with respect to the deployment of EMV-chip cards, according to statistics published by EMVCo. Even outside SEPA, there has been great progress in this respect, with adoption rates exceeding 50 percent in the majority of geographical areas in 2018. The top three types of card-present fraud are:

- Counterfeit card fraud – performed by cloning the magnetic stripe of a card, particularly to spend money outside SEPA in countries where EMV standards have not yet been implemented.
- Lost and stolen card fraud – primarily lost cards being used to perform unauthorised card transactions. The theft of physical cards has also been noticed but to a lesser extent than lost card fraud.
- Identity theft/takeover – fraudsters impersonate the genuine cardholder and make use of their personal information to carry out unauthorised card-present transactions. This category of fraud may overlap with other categories such as counterfeit card fraud or lost and stolen card fraud.

Evolution of the value of fraud by category at ATMs and POS terminals (ECB: 2016)



As in previous years, counterfeit card fraud in 2016 mostly involved transactions acquired outside SEPA. 94 percent of ATM counterfeit card fraud and 79 percent of POS counterfeit card fraud concerned transactions acquired outside SEPA. The total value of counterfeit card fraud decreased by 8.8 percent in 2016.

In 2016 two geographical categories saw decreases in counterfeit card fraud compared with the previous year, namely domestic counterfeit card fraud (by 13.85 percent) and to a smaller extent cross-border counterfeit card fraud acquired outside SEPA (by 9.76 percent). The latter was most likely due to the fact that migration to the EMV security standard was still ongoing in countries outside SEPA.

CNP FRAUD

Card-not-present (CNP) fraud, which nowadays covers mainly "online fraud", has become the most prominent type of card fraud. According to the ECB, the total value of CNP fraud increased by 2.1 percent compared to 2015, reaching €1.32 billion. CNP fraud accounted for 73 percent of the total value of card fraud losses in 2016. This share has been growing steadily since 2008. An increase in CNP fraud of 66 percent over a period of five years was the main driver for the 35 percent increase in overall fraud over this period.

By individual country, France (72.5 percent), the UK (72.3 percent), the Netherlands (68.2 percent), Denmark (39.6 percent), Norway (70.7 percent) and Sweden (48.6 percent) show a significant market share of CNP fraud.

Growth in the number of online merchants implementing 3D-Secure authentication (Verified-by-Visa, MasterCard SecureCode, American Express SafeKey, JCB J/Secure) has gained momentum. However, these anti-fraud measures seem to have contributed only to a slowdown in CNP fraud loss growth rates. Generally, Strong Customer Authentication for remote payments is still underdeveloped from a global perspective.

This is going to change with the implementation of Strong Customer Authentication according to the Regulatory Technical Standards (RTS SCA) of the revised Payment services Directive, PSD2, effective from September 2019.

Interestingly, Visa and MasterCard have announced that they will be starting to move away from traditional 3D secure methods to more use of 3D-Secure 2.0 security with one-time-passwords, EMV tokenisation security and biometrics. However, so far 3D-secure has suffered with a lack of uptake and resistance from consumers and online merchants that fear abandoned payment transactions. That said, these moves by the card schemes show how seriously they take the need for additional verification.

Merchant's view of online card fraud

Distinct from the payments industry, merchants often have their own classification for online card fraud based on fraudulent cases observed in their online shops:

CLEAN FRAUD

where criminals obtain genuine cardholder details including 3D-Secure and Address Verification credentials, along with other information. It is almost impossible for merchants to recognise that the individual using the card fraudulently is not the bona fide cardholder.

IDENTITY THEFT

where the fraudster makes use of the cardholder's personal data in order to make an unauthorised transaction. This fraud can also be categorised as "lost or stolen" fraud since customer card details are stolen and used to purchase goods and services online for the purpose of resale, for example. This type of fraud partly overlaps with clean fraud.

FRIENDLY FRAUD OR FIRST-PARTY FRAUD

where the payer, after having performed a genuine transaction to purchase goods or services online, contacts the card issuer to claim that they have been defrauded and request a chargeback. This type of fraud has reportedly been growing in recent years.

From a merchant perspective, the following fraud and risk management services are seen as the most effective for detecting and preventing e-commerce fraud:

- Card Verification Code (CVV, CVN, CVC2, CID, etc.)
- Address verification service (AVS)
- Negative/blacklists – including those provided by the international card schemes as well as internal lists within the organisation/merchant
- Fraud scoring models
- Geo-location
- Customer purchase history
- Device fingerprinting
- Email verification
- Strong customer authentication (SCA) to be compliant with the PSD2
- 3-D Secure (disliked because consumers often cancel payments when required to use 3D-Secure)

The Changing Face of Fraud

Reporting European card fraud losses and basic fraud details by individual country is only one part of the never-ending fraud combat story.

New fraud trends and digital challenges are hidden behind high-level fraud reporting on card payments. The higher use of digital payment services, the popularity of online shopping and its frequency, different forms of payment and their digital versions, consumers embracing mobile devices and social media networks, and fewer possibilities for customer verification due to open borders are all things that make fraud prevention more complex.

Also, GDPR, Strong Customer Authentication and friendly fraud are mentioned as factors that further complicate a fraud specialist's job. The basics stay the same, but the environment of fraud prevention is ever changing. That means fraud analysts need to be agile, creative and adaptive - just like fraudsters.

For European payment card issuers and payment service providers, the fraud picture has changed dramatically in recent years. In fact, the implementation of EMV Chip and PIN was just a starting point which has changed the whole game – for payment service providers, processors and also for the criminal fraudster fraternity.

The rise in online payments has drastically increased the scope for fraud beyond cards, ATMs and POS terminals. In addition to counterfeit, lost and stolen, mail not received fraud (intercepted cards), ID fraud (theft of card credentials and account takeover) and False ATM Fraud – criminals have invented new types of fraud such as:

- **Phishing, Pharming, Hacking and Carding** (Carding is a form of credit card fraud in which a stolen credit card is used to charge prepaid cards)
- **3D-Secure fraud** when static password
- **Device manipulation:** POS terminal breaches, ATM breaches, consumers' PCs and mobile phones
- **Data breaches** into processing infrastructures or other places with large card data storage (such as merchants and social media networks)

The evolution of payment fraud and organised crime include:

- From petty criminals towards organised global crime industry with decentralised organisation
- From skimming of a single card towards large data breach attacks
- From local fraud towards global fraud organised by decentralised international criminal gangs
- From one criminal working across the entire fraud lifecycle to fraudsters specialising in one part of the value chain, and selling that value on to the next level – for example, one part of the fraudster chain could specialise in getting hold of card data, and another specialises in actually using it
- Device spoofing, location manipulation, threats and bots and business fraud
- Fraudsters masquerading as customers
- Fraudsters concocting perfect fraudulent digital identities
- Global crime rings and lone wolf fraudsters offering Fraud-as-a-Service (FaaS)

In a post data-breach world, identity information, payment credentials, account credentials and responses to security questions are widely available for purchase in bulk. Complete fraud exploits and zero-day attacks are also easily available on the black market for outright purchase or as a hosted/fully managed service.

Worryingly, these fraud offerings come with online help and full technical support. At the same time, the online business environment is becoming increasingly competitive with tighter economics of operation and declining average revenue per user.

If identity data is the critical currency for cybercriminals to perpetrate successful fraud attacks, then trust must be the critical currency for payment service providers. There is a good reason: according to Accenture, digital business will account for 25 percent of the world's economy by 2020.

Fraud cases like "Heartland US" and "Spain 2009" demonstrate that organised high-tech criminal attempts to defraud cardholders and banks have instigated higher levels of fraudulent activity. This can be seen as a kind of new criminal cyber war challenge.

The payments industry therefore continuously demands higher levels of fraud prevention services and security technologies. Consequently, active risk management is mandatory to fight online fraud on the internet and on mobile devices. Furthermore, fraud and risk prevention services must adapt anti-fraud measures on a day-to-day basis.

Fraud as an international organised activity requires cooperative fraud prevention measures including the use of integrated fraud and risk prevention services which incorporate modern modelling techniques. These techniques can be rapidly adapted to respond to attacks and include higher levels of IT security and international standards combined with strong authentication.

Following the worldwide growth of digital commerce, always connected mobile consumers, the high growth rate of online

and mobile payment fraud and new organised crime data breach activities, fighting fraud is mandatory for all payment service providers and their supporting processors.

In a digital payments and post data-breach world, the evolution of card fraud and card-less payment fraud has gained significant momentum. Thus, fraud and risk prevention grows increasingly complex, with higher investments required to cut fraud costs, chargebacks, disputes, and risk management costs.

Fighting fraud can only be done with the right information, though. At this point, no merchant, payment service provider or bank has all the data to determine if a purchase is done by the customer or a fraudster. But combining all the data means a payment service provider would have (almost) all of this information. The challenge is to exchange this data quickly and safely, so the customer is not distracted by the process during their purchase and their privacy is respected.

However, there is good news. Just as fraudsters and cybercriminals learn, improve and innovate, so do payment service providers and their supporting processors. Payment businesses can benefit from the dedicated fraud and risk management services of pan-European processors that combine the latest fraud prevention tools with comprehensive fraud and risk prevention services, managing fraud cases and fraud data across borders at a pan- European level.

Evolution of the Crime Landscape

	1980	1990	2000	2010	2015	2020
Fraudsters	Individuals	Teams	Local crime rings	Global crime rings	"Global crime rings with decentralized organization"	"Global crime rings with decentralized organization"
Target	Consumers	"Consumers SME retailers"	"Consumers Larger retailers"	"Consumers SME/large retailers Issuing Banks Processors"	"Consumers Retailers, Processors, Payment Service Providers, Online Merchants Service Providers, Online Booking Agencies, Payments Industry"	"Consumers Retailers, Processors, Payment Service Providers, Online Merchants Service providers, Online Booking Agencies, Payments Industry ASPSPs, PISPs"
Leading fraud types	Lost/stolen, Intercepted	"Domestic, counterfeiting/ skimming"	Identity theft, Phishing, Rudimentary data compromise	"Cross-border data compromise, CNP fraud, 3D-Secure Fraud, ATM fraud, Identity Theft"	"Cross-border data compromise, CNP fraud, lost & stolen fraud Identity Theft Pharming, Hacking"	"Cross-border data compromise, CNP fraud, lost & stolen fraud, Digital Identity Theft Pharming, Hacking ... Masquerading as customers"
"Type of payment credentials targeted"	Travel & Entertainment cards	"Premium credit cards"	"Mass market credit cards"	"All card types: credit cards, debit cards, prepaid cards"	"All card types: credit cards, debit cards, prepaid cards; bank accounts, apps Online Banking"	"All card types: credit cards, debit cards, prepaid cards; bank accounts, apps Mobile Banking Digital Identities"
Necessary resources	Opportunism	Rudimentary knowledge	"Technical knowhow"	"Audacity, Technical expertise, Insider information, Global connections"	"Audacity, Technical expertise, Insider information, Global connections"	"Audacity, Technical expertise, Insider information, Global connections, Digital Identities, Consumer data from multiple touch point"

Source: Visa Europe, PCM research

4

New Customer Behaviour

In addition to the changing face of fraud, the evolution of cybercriminal capabilities and the complexity of digital omnichannel payment services, another challenge for card issuing banks, payment service providers and processors is the always-connected consumers. The digital consumer now embraces mobile devices and their omni-channel behaviour while shopping and using social media networks.

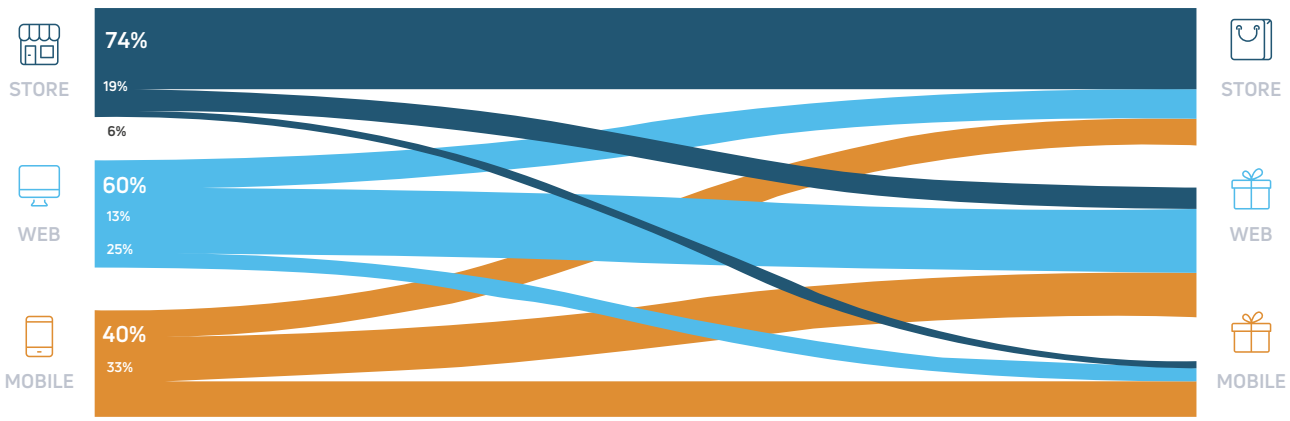
Today's consumers have embraced tablets, smartphones, wearables, messenger apps and social media. This significantly impacts their shopping and payment experiences. Consumers have started to purchase anywhere, at any time, from any device, from any channel, and using the payment means of their choice.

According to retailer associations, the consumer expects a seamless omni-channel shopping and payments experience combined with added-value. Their use of connected mobile devices is seen as a game changer. In 2018, around 70 percent of merchants said that they made at least half of their total sales in the mobile channel.
Driven by the development of social media and mobile devices, the emergence of permanently connected consumers has impacted their interaction with brands but also their expectations of how to shop using the increasing number of touch points and checkouts between consumer, retailer and social media platforms.

European consumers can shop more quickly and easily using mobile devices in many new shopping environments:

- In-store mobile device usage to look up product and pricing information, purchase and payment in-outlet:
  - Look up prices in online shops and, in some cases, approach the merchant for a better price
  - Purchase at a different online merchant, if price in the retail outlet is not competitive or product not available
  - Instant savings and communication with Bluetooth Low Energy beacon or QR-code
  - Self-checkout or in-cart checkout – combined with automatic payments
- Online purchase in online shops – while at home, in-store or away from home
- In-app purchase and payments using QR-codes to bridge from posters to the merchant's online shop
- Click & collect – online purchase with delivery and payment in outlet or by postal service

The shopping Journey of connected consumers



In addition, consumers demand to be able to use multiple payment use cases beyond cards:

- In-store payments with mobile devices:
  - IBAN-based in-app payments directly from the bank account (e.g. HCE NFC, 1D-barcode, QR-code)
  - Mobile HCE NFC payments on cards using digital wallets (Apple Pay, Google Pay, Samsung Pay, MasterPass, Visa Checkout, PayPal)
  - Payments with messenger apps (e.g. Alipay, WeChat Pay), initiated by QR-code or 1D-barcode
  - One-click checkout with automatic invisible payments and conversational commerce, but supported by strong customer authentication
  - Online buy-buttons with one-click payments (e.g. Facebook, Google, Amazon), but supported by strong customer authentication
- Online payments on cards, from bank accounts, or using messenger apps (e.g. Alipay, WeChat App)
- Cash-in-shop banking – cash-in/cash-out per mobile app directly to/from bank account

Changing consumer technology, new consumer behaviours, and consumer protection service expectations are going to challenge the existing in-house fraud and risk management of the individual payment service provider:

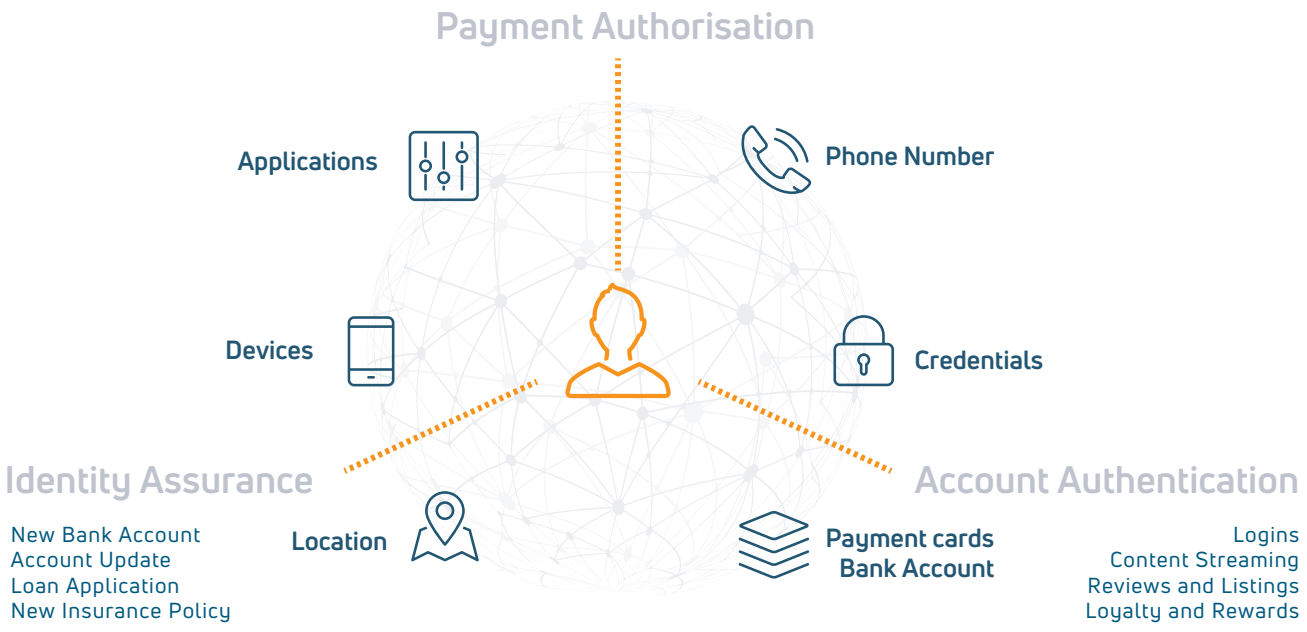
- Connected consumers (mobile, always online, digital natives) use multiple touch points on the internet
- Consumers expect multiple payment services omnichannel from their payment service providers
- Consumers frustrated from (to date) defragmented manual dispute journeys
- Consumers expect online dispute management support added to their mobile banking app
- Consumers expect more consumer protection services from their payment service providers
- Threat: Untrained consumers are insensitive regarding data security and their digital identity data
- Threat: Consumers signing up for subscriptions without being aware they have done so
- Manage new compliance requirements (KYC, eIDAS, GDPR, PSD2)
- Make use of existing national Digital ID services managed by national central banks
  - In the Nordics: NemID (DK), BankID (N), BankID (S), also: IDIN (NL)
- New levels of fraud and risk management expertise required for in-house staff
- Growing workload managing automatic client onboarding and chargeback/dispute services
- Combat new types of fraud, including false digital identities and fraudsters masquerading as customers

From a fraud and risk management perspective, the digital identity of individual consumers in the on-line ecosystem has five dimensions that invite fraudsters to attack:

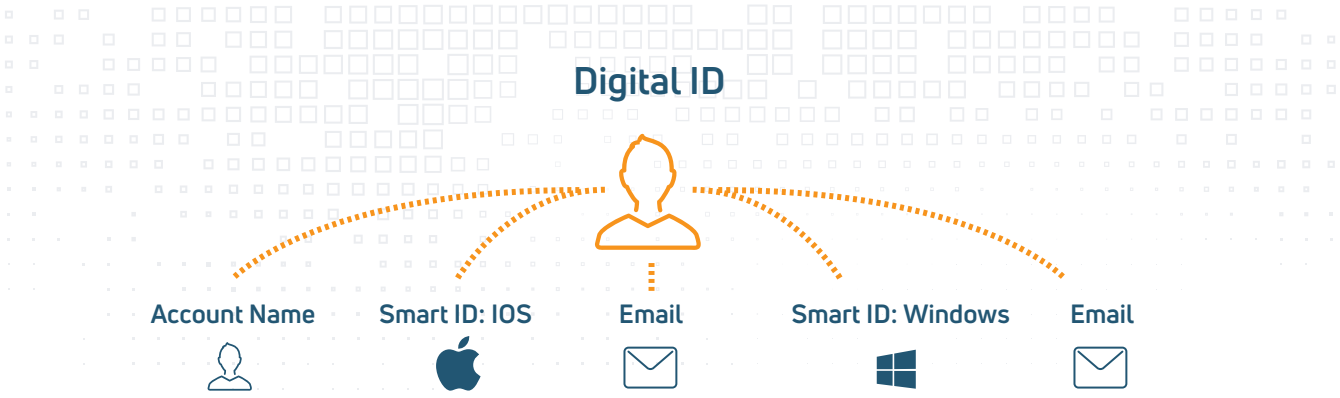
- Personal identity
- Locations
- Devices used
- Threats/Bots
- Payment and business behaviour

Especially, all ID identifiers shall be removed or significantly changed

Consumer touch points in the digital economy



Example for a digital identity from a fraud & risk perspective



Digital transactions continue to form a growing and integral part of many consumers' daily lives. However, this landscape presents fraudsters with a unique set of circumstances to perpetrate cybercrime: an 'anonymous' user, the ever-increasing availability of stolen and spoofed identity data, and the onus on businesses to drive real-time decision making. In 2019, identity data is the critical currency for cybercriminals to perpetrate fraud attacks.

However, payment service providers and their processors learn, improve and innovate to combat fraud. They are aware that identity data is mission critical for their business, too. For example, the use of machine learning in identifying and mitigating fraud has grown by 13 percent since 2015.

A key question for comprehensive fraud and risk prevention services at a European level is how to manage the various touch points of consumers and their individual digital identities in the context of SCA and regulatory requirements such as GDPR
A unique 'anonymous' identifier for every consumer on the fraud and risk management network may be a fitting answer.

5

New Fraud Trends

According to the traditional view of the ECB, there are four significant card fraud trends for the SEPA region:

- Counterfeit fraud is decreasing due to the implementation of EMV chip cards
- Compromised cards and subsequent fraud created outside EMVchip countries
- Card-not-present fraud continues to increase
- Organised crime activities target weak point sectors, processing infrastructure, and environments

As EMV has become widespread, the traditional avenues for card fraud have become dead-ends for fraudsters who are now targeting industries with weaker defences, including social media, store-branded cards, e-commerce and digital identities.

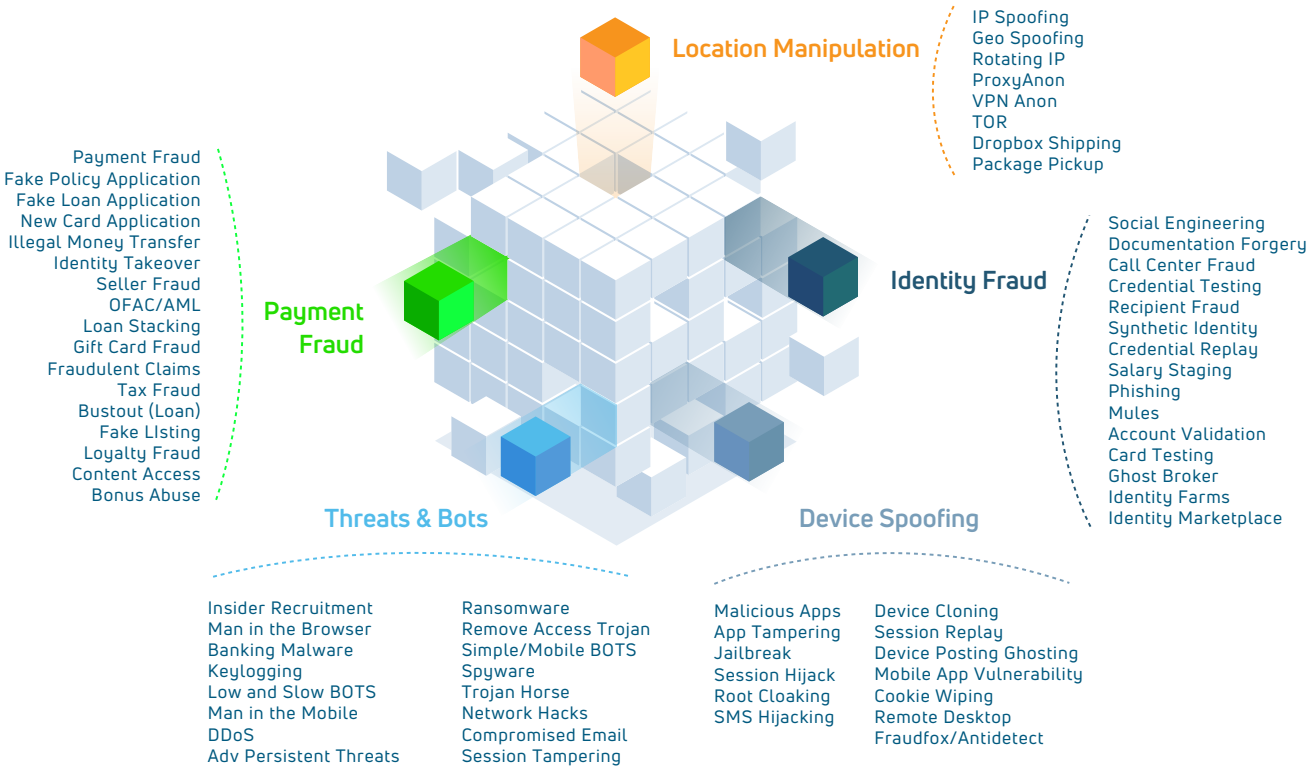
However, the changing face of fraud is driven by fraudsters operating on an international level. They target cardless payments and businesses. Fraud on the internet is a particularly lucrative and low-risk area for criminals as they can operate out of safe havens, and thus are difficult to prosecute.

Obviously, fraudsters follow digital consumer behaviour, and they are always looking for the weakest link and new ways of making profit. Indeed, the digital identity of individual consumers is the mission-critical currency of fraudsters and cybercriminals.

Criminals use a wide range of methods to commit fraud and have a collection of sophisticated fraud types, threats and bots at their disposal. The theft of personal and financial data through social engineering and data breaches was a major contributor to fraud losses in 2018. Stolen data is used to commit fraud both directly and indirectly. For example, compromised card details are used to make unauthorised purchases online and personal details are used to take over an account or apply for a credit card in someone else's name. Criminals also use personal and financial data to defraud customers, using information gained about an individual to add apparent authenticity to a scam.

The graphic below highlights the emerging portfolio of fraud attack capabilities used to penetrate fraud on digital identities of consumers and businesses.

Types of attacks on digital identities



However, UK banks and card companies prevented £1.66 billion in unauthorised fraud in 2018 alone. This represents incidents that were detected and prevented by firms and is equivalent to £2 in every £3 of attempted fraud being stopped. Especially in the Nordic region, card issuing banks and payment service providers help to keep payment fraud at a low level.

Drilling down into new fraud trends, consumers, merchants, banks, payment service providers and processors often have different ways of describing fraud cases. For illustration purposes, this report highlights a selected set of recent fraud cases based on the expertise of fraud experts specialised in day-to-day fraud and risk management:

Contactless Fraud – According to the Danish central bank, DNB, fraud patterns have changed gradually along with the prevalence of contactless payments. Numerically, contactless fraud constitutes a larger share than this technology's share of total payments. In terms of value, contactless fraud constitutes a smaller share. The major part of the amount comes from fraud with chip payments.

Phishing Fraud – One of the big challenges the payments industry faces is an increase in efforts by criminals to deceive consumers into giving away their card data and personal bank account information. Criminals attempt to acquire sensitive information such as usernames, passwords and credit card credentials by pretending to be a trustworthy entity in an electronic communication. The stolen payment data is then used for fraudulent cross-border purchases.

Fraudulent Account Opening and Account Takeover – A fraudster using stolen login details to purchase from a legitimate user's account. The most damaging form of fraud in terms of reputation damage for a business. The social sharing of a hacked account can be expensive to recover from.

Terms of Service Abuse – Customers, often legitimate, attempt to re-use vouchers, sharing vouchers, or seeking to exploit a generous returns or disputes policy. This is the most expensive fraud in terms of operations expense as there are phone calls and investigations to conduct.

Chargeback Fraud – Typically, a user using stolen payment details to purchase goods. Easily the most damaging form of fraud from a financial point of view. Can grow to greater than 2 percent of all transactions if left unchecked or using just a single fraud tool on PSP processor level.

Supplier and collusion fraud – A supplier working with a willing accomplice to accept stolen payment details for large orders knowing they will be charged back. Most expensive in erosion of trust in the marketplace community. This kind of fraud is also expensive to investigate.

About consumers

'Too Good to be true deals', and signing up for subscriptions without knowledge

Too Good to be True Deals – Criminals are targeting consumers directly through social media channels. Scams on social media are nothing new, but they are evolving constantly and share a similar aim: to take advantage of unsuspecting victims online. 'Scam clickbait' is one such example. This practice involves offering the consumer deals too good to be true, e.g. smartphones, television, gift cards, diet pills, skincare products etc.

The clickbait deal is offered under two guises. One scam entices the consumer with legitimate products at an unfeasibly low price. But once ordered and paid for, the consumer never receives the product.

Since it is such a small amount, consumer often overlook it as unimportant, or classify it as too insignificant to report to their banks or the police.

Recurring Payments – Another 'scam clickbait' promotes products such as diet pills or skincare items which are promised to be sent to the consumer for the cost of shipping only. In these cases, even though the product is much more likely to reach the consumer, the purpose of the scam is different: it is intended to persuade the consumer to initiate a transaction that exposes the card credentials.

By accepting the cost of shipping, the consumer must as well agree to a subscription fee. However, the terms of the subscription are usually hidden in the terms and conditions or in very small print, often at the bottom of the page.

Once the consumer has executed the first transaction, recurring transactions will follow, usually bi-weekly. Unsolicited recurring payments operate in a similar way, but fly under the radar. These subscription costs usually low value. Unless the consumer pays close attention to their card statement, they will be charged indefinitely.

From 2011, unwanted recurring payment transactions have increased dramatically. In the Nordic region, 20 to 25 percent of card dispute cases relate to unwanted subscriptions, so-called subscription traps.

The deceptive nature of this crime means that once the consumer has accepted the charge, it becomes difficult dispute, particularly when trying to establish who bears the liability, the bank or the consumer?

One reason for this is that with scam clickbait fall into a grey area, as the consumer has voluntarily provided its payment details to the merchant. In addition, merchants and acquirers have applied the card scheme rules.

Merchants, acquirers and payment service issuers cooperating cross-borders with their processors and the police forces have detected and stopped a kind of cybercriminal supply chain of the so-called dark economy composed of the following five successive steps: data breach, online purchases with stolen card credentials, anonymous collection of products and repacked delivery services, followed by online sales out of fraudulent online shops.

High Tech Data Breach and Automatic Attacks – A specialised high-tech fraudster team hacks into a retailer or bank with lower fraud control levels. The hackers use a Trojan horse-type virus to steal thousands of valid card credentials and/or other payment data. This data is then sold on the internet to fraudsters or other criminals of the so-called underground economy.

According to IBM Security and its '2018 Cost of Data Breach Study', the average total cost of a data breach, the average cost for each lost or stolen record (per capita cost), and the average size of data breaches have all increased:

- The average total cost rose to $3.86 million, up 6.4 percent over 2017
- The average cost for each lost record grew to $148, up 4.8 percent over 2017
- The average size of data breach increased by 2.2 percent over 2017

Online purchases with misappropriated cards – Fraudsters buy large volumes of products online (such as attractive electronic devices) from online merchants. Payment is made using fraudulently obtained card data and/or other payment data from data breaches. Mostly, cardholders are not caused financial loss as credit cards allow for dispute of the fraudulent use.

Anonymous Collection – The fraudulently purchased products are delivered by bona fide online merchants to fraudulent delivery addresses, such as unattended freight stations, drop zones, and fraudulent small merchants.

Repacked Delivery – After repacking, and again using unattended freight stations (drop zones), the fraudulently purchased products are delivered to unaware online buyers who assume the seller is bona fide when buying the products on internet auctions.

Online Sales out of fraudulent online shops – The fraudulently purchased products are offered to online buyers on internet auctions websites or in fraudulent online shops ("Too good to be true price") which act as receivers of fraudulently purchased goods.

Beyond the well-known payment fraud, fraudster activities show more sophisticated attacks to scam and use digital identity information of consumers and businesses:

Fraudsters masquerading as customers – The world of cybercrime continues to evolve quickly and many businesses are struggling to keep up with the pace. Fraudsters have evolved their tactics from single-point attacks on end user accounts to multifaceted attacks that incorporate multiple vectors for many varied purposes. Central to the success of these attacks is the ability for fraudsters to masquerade convincingly as trusted customers; so much so that their transactions have become almost indistinguishable from legitimate ones. It's a challenging battleground.

Device spoofing – These techniques are widely used by fraudsters to evade device recognition and detection capabilities. Device spoofing allows a fraudster to masquerade as a legitimate customer, manipulate login sessions, open fraudulent accounts, intercept user credentials or take advantage of multiple new account bonuses.

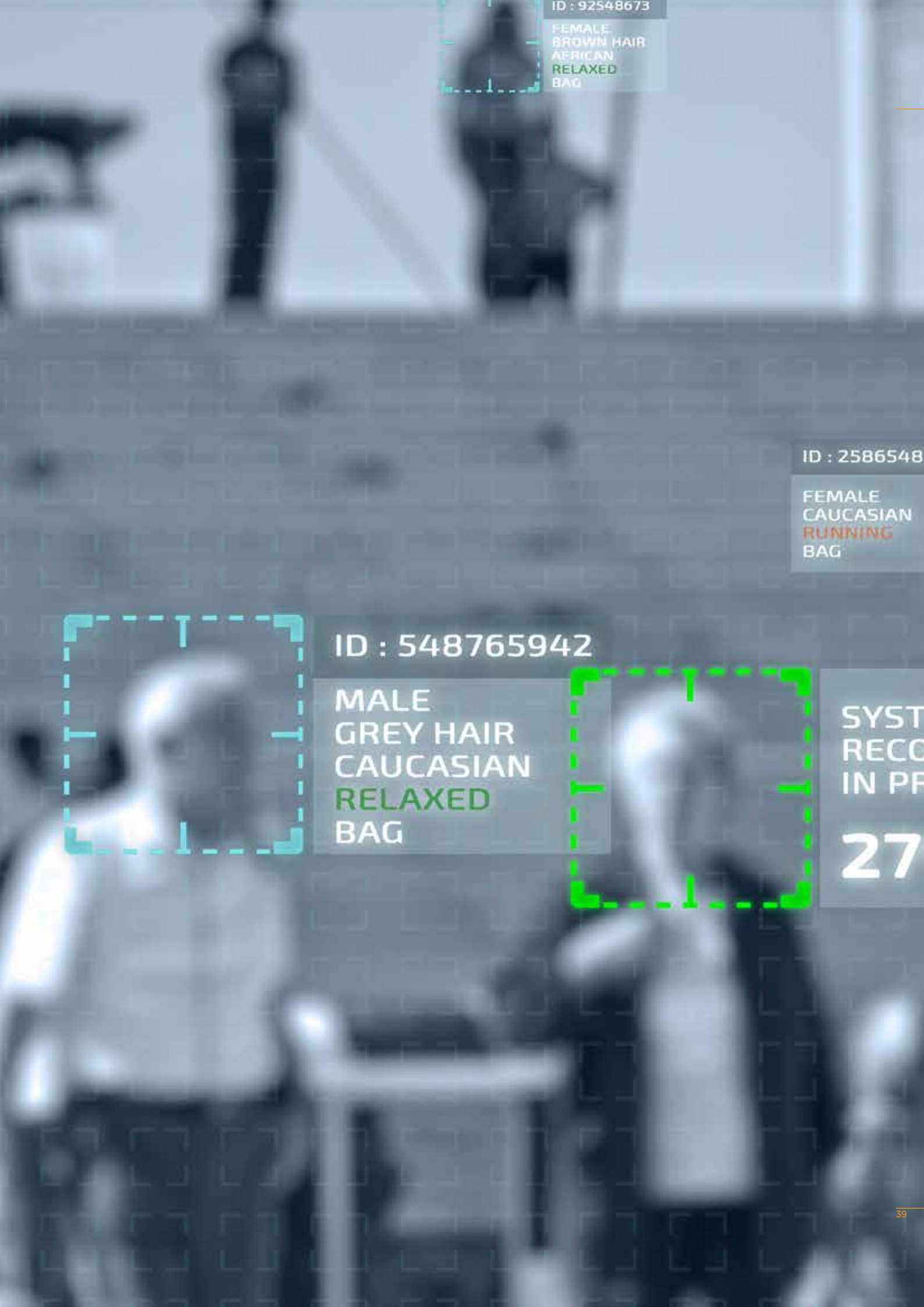
Location manipulation – Fraudsters manipulate their location tracking in order to mask their true whereabouts. Sometimes this allows them to pretend to be a legitimate customer, or to trade from a location that is perhaps blocked by a company's business rules or banned under regulatory compliance such as the anti-money laundering directive (AMLD).

Identity Fraud – Fraudsters are creating complete identities using a patchwork of stolen identity data, harvested from data breaches and the dark web. These stolen and spoofed identities are often a near-perfect match for the a "real" identity, and are used to open fraudulent new accounts, takeover existing accounts and monetize stolen credit cards.

Threats and Bots – Fraudsters have a collection of threats and bots at their disposal to perpetrate fraud, including Malware, Remote Access Trojans (RATs), Man-in-the-Middle attacks and automated bot attacks. These are often used in combination to perform mass identity testing attacks (via an advanced bot), and then take over a trusted user account via a Man-in-the-Middle attack and/or RAT.

There is no doubt that the new fraud trends bring more complexity to combatting fraud. In addition, ongoing enhancement of fraud and risk management services is a key challenge for card issuing banks and payment service providers (see below).

According to leading fraud and risk prevention service providers, it would be a winning strategy for banks and payment service providers to use services which support protection for the digital identities of consumers and business.


ID : 92548673
FEMALE
BROWN HAIR
AFRICAN
RELAXED
BAG
ID : 2586548
FEMALE
CAUCASIAN
RUNNING
BAG
ID : 548765942
MALE
GREY HAIR
CAUCASIAN
RELAXED
BAG
SYST
RECO
IN PR
27

6

Key Challenges for Banks and Payment Service Providers

The complexity of effective fraud prevention has increased significantly in recent years. Digital payments and data breaches here are significant challenges for card issuing banks, payment service providers and processors. Firms across all industries must bolster their defences against new account fraud while simultaneously developing their digital service capabilities

Banks and payment service providers are clear that defending and protecting digital identities for consumers and businesses is the most essential part of omni-channel fraud and risk management services for the decade ahead.

In parallel, consumers continue to demand robust online and mobile channels for everything from enrolment to payments, from banking transactions to consumer protection in the digital economy. This means that banks, payment service providers and processors need to provide a frictionless customer service experience across cards, cardless transactions, omni-channel, Open Banking and more.

This report highlights the key challenges for banks and payment service providers as identified from interviews with fraud experts and key industry players:
Changing Technologies – Apart from providing ongoing high-levels of data protection and cyber security, the changing technologies challenge legacy systems. Examples include mobile, digital, 3D-Secure 2.0 and EMV tokenisation.

Due to changing technologies, digital consumer demands and new fraud trends, legacy systems are often seen as no longer adequate to respond to the latest risk management demands. Finding the best combination of services is a challenge, considering a company's budget, availability of staff and their knowledge level and experience.

Ultimately, cybercriminals may manage to bypass new security techniques, so it is essential that even the strongest types of security are underpinned by intelligent omnichannel fraud prevention services that can learn and adapt as fraud changes, and which can be very easily updated to respond to changing threats when they happen.

Common Card Fraud Prevention Measures Practiced

Type of Misuse	Prevention Measures	Developments
Domestic/International transactions at EMV POS & ATMs	• EMV with DDA/CDA, PIN-only, SMS notification • Cardholder awareness	• DDA to CDA • Dynamic authentication
International transactions in non-EMV POS & ATMs	• Prevention of initial data capture – Merchant (skimming protection, PCI DSS – ATM security (skimming protection) • Issuer and acquirer monitoring: – Card use, rule-based fraud prevention – Major locations of POS & ATM fraud • Cardholder awareness (pre-notification of international travel, SMS notification)	• Global EMV Rollout, includes now USA • Dynamic authentication • Chip only cards (e.g. V PAY) • Geo-blocking, card limits • phase-out magstripe • processing of EMV cards
Card-not-present, especially online transactions	• Prevention of initial data capture: – Merchant (PCI DSS), – ATM security (skimming protection) • Card Security Codes (e. g. CVC2, CVV2, CID, CID2) • 3D-Secure 2.0, one-time authentication code, tokenisation • Cardholder awareness (use of anti-virus software, secure websites, transaction alerts, etc.)	• Dynamic one-time authentication codes • Geo-blocking, card limits (e.g. Maestro cards) • Tokenization + HCE NFC • Digital Wallets • Device locations

Source: PCM research.

The common card fraud table highlights basic card fraud prevention measures to mitigate risks having strong customer authentication in mind:

Compliance with the legal framework for payment services – In all banks, compliance is at the top of the agenda, meaning that a certain level of fraud sometimes becomes accepted because of IT limitations. Thus, payment servicing banks risk higher costs from liability shifts of non-compliant payments to their balance sheet.

The General Data Protection Rules Directive, GDPR, and compliance with Strong Customer Authentication relating to PSD2 are factors further complicating a fraud specialist's job. The basics stay the same, but fraud prevention is always changing.

Consumer Protection – Consumers demand protection from financial loss as well as from unpleasant experiences leading to dissatisfaction with card payments, and their bank. Consumers also expect protection from the inconvenience of having to file a dispute with merchants.

Digital Identity Management – Trust is the critical currency for businesses and the payments industry, while digital transactions continue to form a growing and integral part of many customers' daily lives. If organisations can genuinely understand who their customers are, and how, when and why they transact, then companies will spot the infiltration of unusual and anomalous behaviour more rapidly. A key question is how to manage the omni-channel use of various touch points by the consumers and their individual digital identities in the context of SCA and regulatory requirements of GDPR. Banks and payment service providers should reconsider their view on identity, focusing less on static pieces of information that traditionally make up a customers' identity. The challenge is to focus on a wider concept of digital identity that includes personal identity, devices, locations and payment behaviours.

Next Level of Fraud and Risk Prevention Services – The scale and changing profile of card fraud losses underlines the urgency of implementing comprehensive security measures and of reinforcing those measures through use of the right fraud and risk prevention services.

A single fraud prevention solution is not sufficient to fight fraud effectively. Every fraud prevention solution has its own strengths and limitations. A layered approach using several tools can help to capture different types of fraud, but it also implies to 'trust' all tools with a risk of false rejections.

Finding the best combination of services can be a challenge, considering a company's budget, available staff and their knowledge level and experience. In order to circumvent inflexible legacy systems, outsourcing of technology and fraud experts is a solid option.

In addition, it is important to combine the latest fraud prevention tools with comprehensive fraud and risk prevention services which can handle the automatic onboarding of customers, digital identities, dispute handling, fraud cases and fraud data cross-borders across Europe.

In order to keep pace with increasing fraud and risk challenges, banks and payment service providers would need to be clear about a build or buy decision:

- Either invest in the next generation of comprehensive in-house fraud and risk prevention services
- Or benefit from managed all-in-one fraud and risk prevention services covering the latest fraud and risk challenges, while maintaining control of their own data
- Or combine existing in-house fraud and risk management with white-label support to close the in-house gaps.

7

Threats/Weaknesses in existing Fraud and Risk Services

Standard fraud measures are a pre-requisite for the payments industry. However, these no longer represent the full fraud and risk prevention portfolio required.

Platform weaknesses – A lot of payment platforms in Europe do not support multiple payment services in an omni-channel environment. The weaknesses of legacy processing systems and fraud and risk management processes may include:

- Mono-channel payment processing with separated platforms for POS payments and online payments
- No omni-channel payment transaction data available for omnichannel use with fraud and risk prevention
- Manual onboarding of customers combined with fragmented KYC utilities
- Fraud and risk management services rather detect than prevent with separate processes for card payments and for cardless payments
- Fraud and risk prevention is restricted to in-house payments data and in-house fraud prevention rules – for example regional cross-border payments data cannot be used to improve anti-fraud measures
- Limited in-house capability to prevent from threats that come from data hacks on merchant client systems, and system compromises that continue to concern merchants and consumers
- Limited or no digital identity management capabilities, e.g. there are no prevention measures for device spoofing and location manipulation
- Fragmented or manual dispute processes, including long-term response cycles to customer disputes
- Lack of automation in the fraud process does not allow for reducing manual fraud and risk services, e.g. high cost for fast-growing dispute cases
- Limited capabilities for consumer protection services

Finding the best combination of services is a challenge, considering a company's budget, available staff and their knowledge level and experience.

Internal weaknesses may include a lack of resources within organisations, especially personnel with the relevant expertise in fraud detection and prevention (seen as a key issue), gaps in fraud tool functionality and issues related to the speed of response to emerging threats and tracking friendly fraud. Also, there may be a lack of resources for fraud research, investigations in new fraud cases and in co-creation with law enforcement.

A company's compliance workload has priority, meaning that fraud can sometimes become accepted because in-house IT has insufficient capacity.

Dispute Weaknesses – Many banks and payment service providers have fragmented dispute processes, including manual work providing consumers with a timeline longer than demanded. Dispute is a niche, and difficult for the banks to get and maintain sufficient knowledge about scheme rules. Given this lack of knowledge, the bank might decline a disputed transaction when they could have helped their customer.

Based on best practice in the Nordic region, an important objective for banks and payment service providers is to combine the latest fraud prevention tools with comprehensive fraud and risk prevention services that can manage the automatic onboarding of customers, digital identities, dispute handling, fraud cases and fraud data across borders at a pan- European level.


Alt

8

Benefits of a Next Generation Fraud and Risk Service

AN OPEN PAYMENT PLATFORM –COLLECTING OMNICHANNEL PAYMENTS DATA FOR FRAUD PREVENTION USE

A solid basis for next-generation fraud and risk prevention services is an omni-channel payment processing service platform that supports data and security compliance, tokenisation security, payment innovation, secure payment credentials, and a frictionless omni-channel user experience. This kind of platform can also be the basis for collecting huge amounts of omni-channel payments data.

In a digital payment world, Open Payment platforms support the following characteristics:

- Omni-channel payment processing: ATM, POS/MPOS, SmartPOS, online shops, mobile in-store, in-app
- End-to-end payment processing of cards, IBAN-based bank payments, instant payments and other advanced payments
- The latest payment security standards, e.g. 3D-Secure 2.0+, EMV tokenisation, HCE NFC
- Omni-channel payment transaction data at a European level available for use with fraud and risk prevention services
- Payment data from multiple payment services available for fraud and risk prevention tools and services
- Supports real-time authentication and rule-based fraud control covering the latest fraud trends
- Supports fraud control measures such as geo-blocking and channel-blocking for the restricted regional use of payment services
- Enables sophisticated limit management at the merchant level, cardholder level and by payment use case
- Supports digital identity schemes such as BankID (N), BankID (S), NemID (DK) and TUPAS (SF) to secure online payments with digital identity authentication
- Compliance with domestic and EU regulations as well as card scheme rules related to payments

ABOUT NEXT GENERATION FRAUD AND RISK PREVENTION SERVICES

The next generation fraud and risk prevention service capabilities go far beyond just fraud and risk solutions. They strive to prevent rather than detect, which requires research, investigation and collaboration with law enforcement. These systems also combine real-time fraud prevention and neural networks with fraud expertise and integrated supporting services such as automated dispute management and customer protection services.

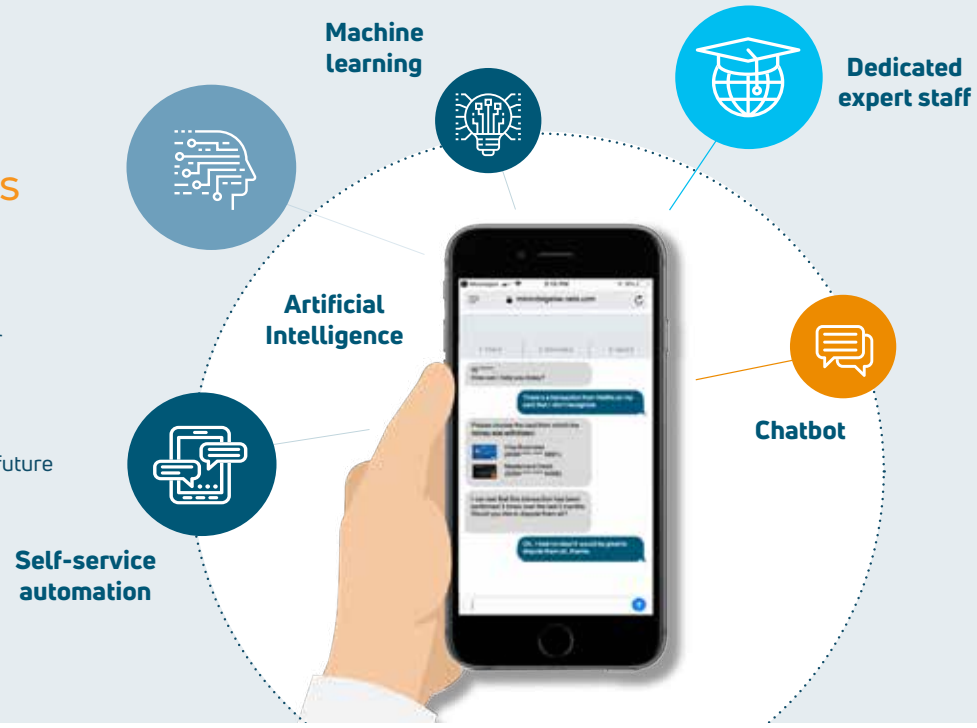
Based on the Nordic best practice of preserving cardholder and payment business trust, the value proposition for next generation fraud and risk prevention services includes:

- Building for the future with the tools to mitigate risk from the latest fraud trends
- Using a framework that provides fewer fraudulent transactions with less card usage restrictions
- Fraud prevention services with benefits from large amount of payments data on a European level
- Instant implementation of measures to combat the latest fraud trends
- Automated processes that reduce the labour costs of manual fraud and risk services
- Improve automatic consumer and merchant onboarding combined with added KYC utilities
- Support of automated dispute processes, including mobile dispute service apps for consumer disputes
- Credit card protection
- Consumer protection services
- GDPR compliant use of consumer and merchant data
- Contribute to cut fraud cost, dispute cost, and chargebacks cost

Next Generation Disputes Management, automated, efficient and increased customer experience

Benefits to banks

- Market-leading resolution rates
- Up to 40 - 50% reduction in the cost of managing disputes
- Significantly improved customer experience
- Plug and Play – rapid no set up cost
- Future-proofed - committed to future technology enhancements



CUSTOMER VALUE IN NEXT-GENERATION FRAUD AND RISK PREVENTION

Next generation fraud & risk prevention services, when combined with highly skilled experts and state-of-the-art payment processing platforms, can provide significant customer value for banks, payment service providers and consumers.

This report addresses the following seven key arguments:

Fewer fraud and dispute losses – contributing to reduction of fraud losses and less cost for dispute handling as fraud cases, dispute cases and payment transaction screening are instantly managed by highly skilled experts.

Scale of daily operations 24/7/365 – daily operations taking into account the latest fraud trends, always with a one-point-of-contact for banks and their cardholders. Experts prevent fraudulent cases and, in case, notify the cardholder 24/7/365.

Large cross-borders amount of payment data for fraud and dispute analysis – utilising larger amounts of payment data at a European level. Thus, allowing the performance of extensive analysis of fraud and dispute trends cross-borders, leading to better performance.

Cost savings – next generation fraud prevention allows banks to creating synergies by providing fraud and dispute resolution services across the whole value chain. In addition, increased automation reduces the need for manual review.

Regulatory compliance as a white-label service – in order to minimise compliance risks, banks can make use of the white-label expertise of an external fraud and dispute resolution partner to ensure compliance with applicable domestic and EU regulations as well as card scheme rules related to fraud and disputes. These white-label services enable banks to be in control of their own data and deliver state of the art digital solutions to their customers.

Collaboration with authorities and other public stakeholders – customer value due to frequent collaboration with authorities to solve payment fraud at domestic, Nordic, and pan-European levels.

Increasing customer satisfaction – combining a safe and flexible pan-European payment processing experience with modern and efficient fraud management solution contributes to reducing fraudulent transactions and unnecessary disputes and, thus, mitigates risks and minimises possible financial loss.

Next generation fraud and risk prevention services include two value-added unique selling services: Automated Dispute Processes and Customer Protection Services:

AUTOMATED DISPUTE PROCESSES – BENEFITS FOR CARD ISSUERS AND CARDHOLDER

Next generation fraud and risk prevention services include automated dispute management processes with benefits for banks and payment service providers using the service, such as a short user experience timeline which helps to cut dispute costs and reduce chargeback costs.

- Automated process management - a mobile dispute service app from dispute initiation, through follow-up and resolution. This includes services for issuers and card schemes including validation, handling and processing of disputed cases, and as well as final reporting
- Enable card issuers to handle mandatory dispute processing according to applicable scheme rules and local legislation

Success stories of disputed cases are a topic that consumers, cardholders and bank clients share with their friends and families, so it is important to ensure a good customer experience when these cases occur.

CONSUMER PROTECTION SERVICES

By conducting regular in-depth analyses of the available card dispute data at a European level and using markers such as regular business name and acquirer, customer protection services can identify those merchants operating in the fraudulent 'grey zone.'

Part of the role of consumer protection services is to monitor and analyse vast amounts of data gathered through fraud prevention tools, using them to identify potential clickbait-generated transactions, and declining payment transactions in real time.

Tackling financial fraud is another priority for customer protection services. While scams targeting victims with increasingly sophisticated methods remain significant, the problem can be addressed through collecting data on activities between consumers and stakeholders in the financial ecosystem. Financial institutions must prepare to respond to these incidents appropriately, remaining vigilant to the threats against their customers and working with them to stay one step ahead of cybercrime.

The consumer benefits of these protection services are manifold. Consumers are protected from financial loss as well as from an unpleasant experience with a fraud case which could lead to dissatisfaction. These services also protect consumers whose transactions to merchants are declined from the inconvenience of having a file dispute.

Card issuers are also beneficiaries of this service. They experience fewer dissatisfied customers and a significant reduction in the number of fraud cases, incoming disputes and customer complaints.

In the Nordic region, banks utilising these services have experienced a dramatic fall in the number of card disputes. This not only reduces overall operational costs for the issuer in question, but also increases customer satisfaction.

e-ID Systems in the Nordics

Banking, government services and payments increasingly take place online, with a dizzying array of services and platforms. However, unlike the real world, there is no outward face which reveals the true nature of these digital inhabitants. How do we prove that we are who we say we are?

An electronic Identity (e-ID) scheme is the digital counterpart to a physical identification method in the offline world such as a passport, ID-card or driver's license. It provides the credentials necessary to trust that a person is who he/she claims to be online. The Nordic countries have successfully established e-ID schemes, giving their citizens a digital online identity that is recognized both by casual users, and by the most secure authorities in the country. In all four Nordic countries, a solution jointly initiated by a group of banks has taken the dominant position for a clear reason: banks in collaboration have a huge advantage over governmental and third-party solutions as they have a pre-authenticated client base. They are the only players who have already authenticated the majority of their country's citizens and transferred them to online/mobile banking.

The banks in the Nordics see their e-ID schemes as an enabler for their businesses and as a product from which many other services can profit, including online merchants, payment businesses and next generation fraud and risk prevention services. For example, a Nordic rental service provider states that with e-ID, 90 percent of its customers sign their rental agreements online, resulting in decreasing costs, higher sales and stronger margins.

It took Sweden, as the first country to initiate federated e-ID developed by banks, roughly 13 years from launching the first e-ID to having all major banks on board and providing an essential part of daily life for millions of Swedes. Denmark, which started about 10 years later needed only half this time to write its own success story, having learned from the other Nordics.

After initial hesitation, all major Nordic banks issue and support e-ID schemes. They have understood that this enables them to digitalise their business – offering 24/7 service, cutting costs and increasing sales. Furthermore, they have seen the benefits in offering federated e-IDs as a service to third parties and designing new products leveraging on these solutions, thereby digitalising the whole economy.

The Nordic e-ID schemes

A crucial key to succeeding with an e-ID is to gain sufficient critical mass in a two-sided market. Citizens will only see the benefits if there are enough use cases, and the same holds true for companies in need of strong authentication and e-signature services. Any provider who is already active in the Nordic markets, such as a large banking group, has a competitive advantage; they can offer a new service that all their customers, consumer and corporate, benefit from.

Registering for the e-ID in the Nordic region is simple. The Nordic example demonstrates that they did better than providers such as governments and telecommunications companies, as most of their customers already had log-in credentials for online banking.

BANKID
- First issued in 2003
- 8 million users
- 2.5 billion transactions
- Mobile version since 2010

BANKID
- First issued in 2004
- 3.9 million users
- 600 million transactions
- Mobile version since 2009

TUPAS
- First issued in 2003
- 4.7 million users
- Transactions n/a
- Mobile version since n/a

NEMID
- First issued in 2010
- 4.8 million users
- 704 million transactions
- Mobile version since 2018

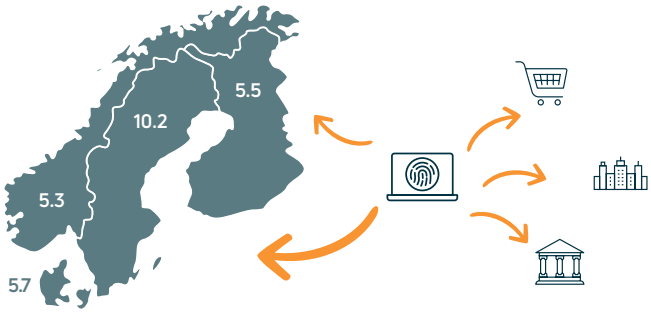
BANKID
- 78% penetration
- On card and file; mobile version App based, independent of bank/SIM card used

TUPAS ID
- 87% penetration
- Each bank has own solution, with shared common interface

BANKID
- 74% penetration
- Bank specific code devices; mobile version bank independent, requires right SIM card

NEM ID
- 85% penetration
- Initially passwords on paper, code app launched May 2018

e-ID as fraud-preventing connector in the Nordic market



9

Key Findings

Card fraud is one of the most fascinating aspects of the payments industry, not least because it is always changing. EMV implementation and 3D-Secure, combined with Strong Customer Authentication, have done much to reduce domestic losses from lost and stolen cards in Europe.

However, higher use of digital payment services, the popularity of online shopping and its frequency, different forms of payment and their digital versions, have all combined to make fraud prevention more complex.

Driven by the development of social media and mobile devices, the emergence of permanently connected consumers has impacted their interaction with brands but also their expectations of how to shop using the increasing number of touch points and checkouts between consumer, retailer and social media platforms.

In the digital payments and post-data breach world, there are significant challenges for card issuing banks, payment service providers and their supporting processors. Firms across all industries must bolster their defences against new fraud trends while simultaneously developing their digital service capabilities.

However, the legacy systems of many banks and payment service providers are challenged as they are often seen as no longer adequate. Standard fraud measures are a pre-requisite, but they no longer represent the full fraud and risk prevention service portfolio required.

The scale and changing profile of payment fraud losses underlines the urgency of implementing comprehensive security measures and of reinforcing those measures through use of the right fraud tools with comprehensive fraud and risk prevention services. These should be combined with digital dispute services, consumer protection services, and automatic onboarding.

Fighting fraud can only be effective with the right information. At this point, no merchant, payment service provider or bank has all the data to determine if a transaction is executed by a customer or a fraudster. By combining all the data from issuers, acquirers and processors, a payment service provider would have the information required The challenge is to exchange and collect this data quickly and safely at a pan- European level, so the customer is not distracted and their privacy is respected.

According to fraud experts and payments industry players, it would be a winning strategy for banks and payment service providers to use services that protect the digital identities of consumers and businesses such as omni-channel fraud and risk prevention services.

Just as fraudsters and cybercriminals learn, improve and innovate, so too do payment service providers and their supporting processors. Payment businesses around the world can benefit from next generation fraud and risk management services based on the best practice achieved in the Nordic region.

Payments businesses should look to the Nordics example and combine state-of-the-art fraud prevention tools with comprehensive fraud and risk prevention services. These services manage fraud cases and fraud data across borders at a pan-European level, and allow for the automatic onboarding of customers and merchants, dispute handling, and customer protection services. Such services have changed the customer perception of payments security in the Nordics and could well do so across Europe.

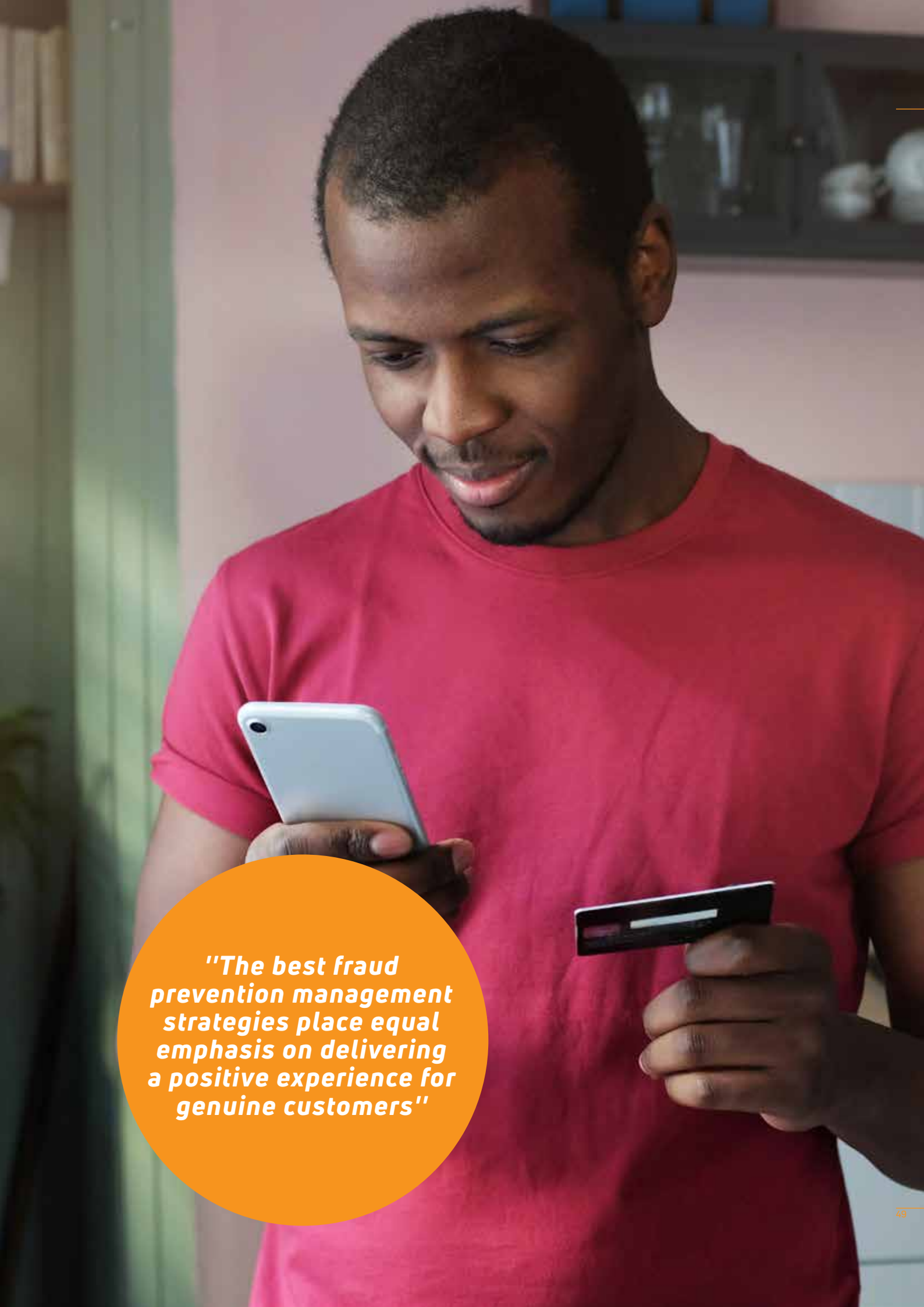
In order to keep pace with increasing fraud and risk challenges, banks and payment service providers have two options:

- Benefit from next generation fraud and risk prevention services managed by a trusted external partner that can cover the latest trends, while allowing payment businesses to keep control of their own data
- Combine existing in-house fraud and risk management with white-label next generation support to close gaps in their in-house services

In both cases, they should select a next-generation service which can contribute to lower fraud rates and cut fraud costs, chargeback costs and dispute costs.

In conclusion, the best fraud prevention management strategies place equal emphasis on delivering a positive experience for genuine customers, accurately detecting and rejecting fraudulent orders, and efficiently managing operational costs associated with fraud prevention.

Companies that achieve a balance between these three factors see significant benefits accrue across their business, including significant lower chargeback rates than other companies, and lower staff costs associated with fraud prevention.



"The best fraud prevention management strategies place equal emphasis on delivering a positive experience for genuine customers"

About The Research

PAYMENTS CARDS & MOBILE

In business since 1994, Payments Cards & Mobile is an established hub for global payments news, research and consulting. We work with recognized industry experts to provide impartial, up-to-date and relevant information and analysis on every area of payments.

Personal relationships have been the hallmark of our business. We remain committed to working closely with our many long-standing customers and welcome new customers in producing quality business intelligence and providing a variety of ways in which you can consume this information. Our aim is to provide you with the highest quality data so you can position your business and key personalities in this increasingly competitive industry.

PCM RESEARCH

Payments Cards and Mobile Research offers comprehensive, in-depth research into topics which are relevant and tailored to our clients' needs. Our in-house research facility is available for short term projects. We specialize in M&A activity, market entry data, country report analysis and statistics. Research reports on banking, payments and mobile payments worldwide.

Topics range across the measurement of efficiency and performance, card and payment service related information, the role of brands in banking and the impact of non-banks such as retailers and FinTechs on the financial services and mobile financial services market.

Payments Cards and Mobile offers specific research on all aspects of banking, card payments, card-less digital payments, Issuing/ Acquiring, financial services and the mobile financial services market.

Nets

Nets is one of Europe's largest payment processors, partnering with more than 240 banks, we initiate transactions from approximately 40 million cards and monitor more than 3.5 billion transactions. This proven expertise and the scale of resources means customers have access to a range of services that ensure safety and stability in their solutions at all times.

By choosing Nets as Fraud & Dispute partner we assist you in ensuring that you are compliant with applicable domestic and EU regulations as well as card scheme rules related to Fraud and Dispute. Our modern and efficient Fraud Management Solution will reduce fraud losses and our highly skilled experts handle dispute cases to ensure high winning rates.

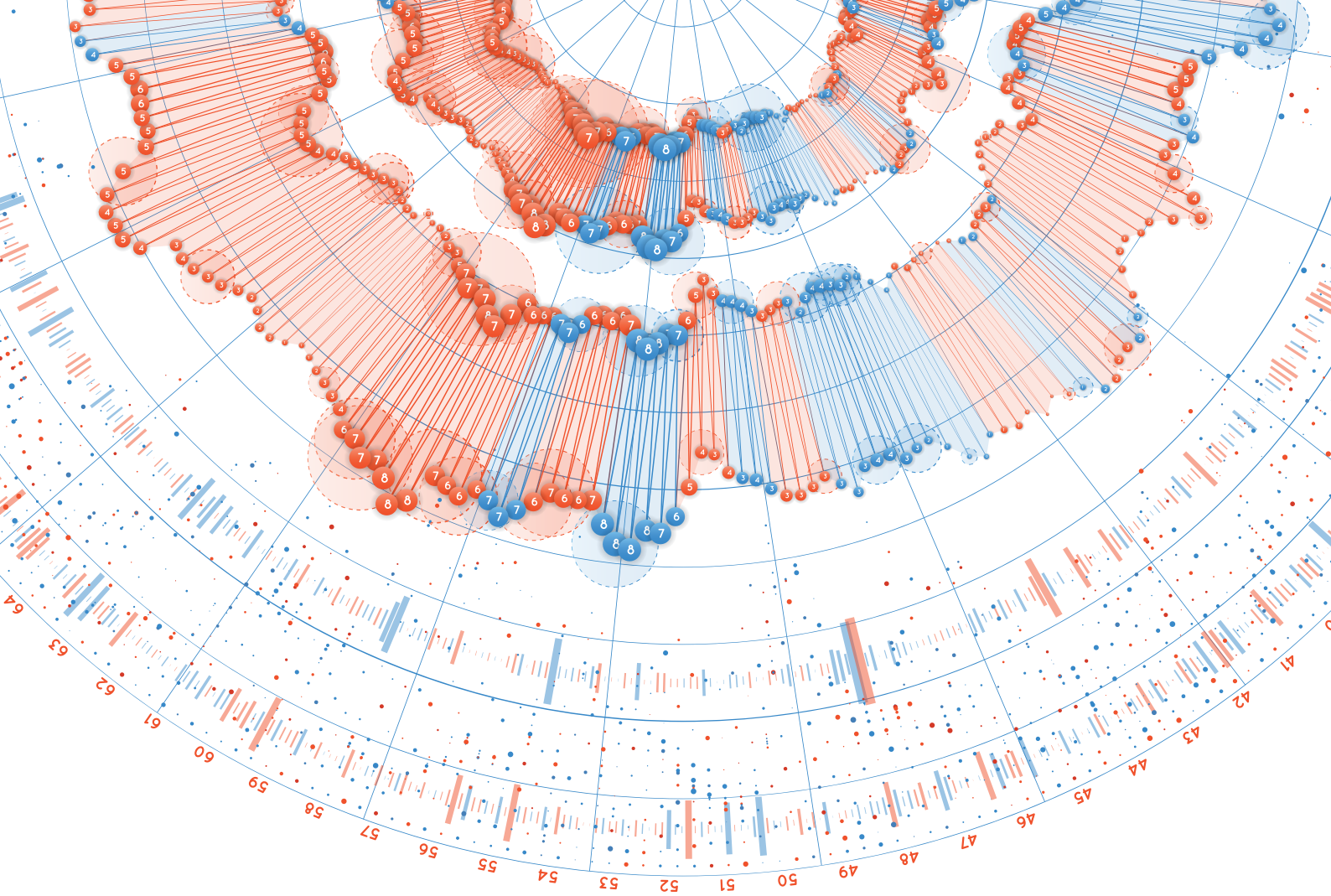
www.nets.eu/solutions/fraud-and-dispute-services

ACKNOWLEDGEMENTS

The study draws on published statistics and on comments from retailers and payments industry players. The author thanks various retail organizations and payments industry companies for the data provided and the helpful responses to selected questions on omni-channel retailing, multi-payment services, and omni-channel payment platforms.

AUTHOR

Since 2011, Horst Forster has been co-editor of the European Payment Cards Yearbook, responsible for market analysis and for compiling/ writing the country profiles. Horst has more than twenty years' expertise in both omnichannel card business and card-less payments. Across business and across borders, his profession is business development and market intelligence services for the payments Industry, including digital payments in an Open Banking ecosystem.



PAYMENTS INDUSTRY INTELLIGENCE

We offer **individual in-depth research reports** for market analysis and strategic business demands.

- Market analysis and country reports – by individual European country
- Acquirer Reports Europe
- Issuer Reports Europe
- Card Processors in Europe
- Internet Payment Service Processors in Europe
- Payment Trends
- European Legal Framework for Payment Services

Bespoke PCM Research on demand

www.**paymentscardsandmobile**.com Call (+44) **1263 711800**

PAYMENTS INDUSTRY INTELLIGENCE
Payments
CARDS & MOBILE

www.nets.eu/solutions/fraud-and-dispute-services

nets