

A map of Europe with various percentage callouts in red and green circles. The callouts include: 6.3%, 0.4%, -5.0%, 21.7%, 0.0%, -2.1%, 6.0%, 0.0%, -2.4%, 2.4%, -1.7%, and -5.3%.

## How Europe's Card Fraud Is Evolving

New data shows the 2014 trends in CNP, cross-border and other fraud types across the region

Track the evolution of European card fraud from 2007–2014

Working with issuers across Europe, FICO has seen big changes in the fraud landscape. These changes are illustrated by new data from Euromonitor International, which show how different countries' defences against fraud, their adoption of powerful analytics and their use of EMV technology have pushed criminals from one country to the next and from one form of attack to another.

This white paper provides a snapshot of these trends for 2014, as well as commentary from Martin Warwick, FICO's fraud chief for Europe.

- Discover which types of card fraud are rising in 19 European countries
- Explore the movement of threats across the region
- See how the forthcoming adoption of EMV standards in the US is impacting European cards
- Learn what issuers should focus on

Figure 1: European Fraud Changes, 2013–2014

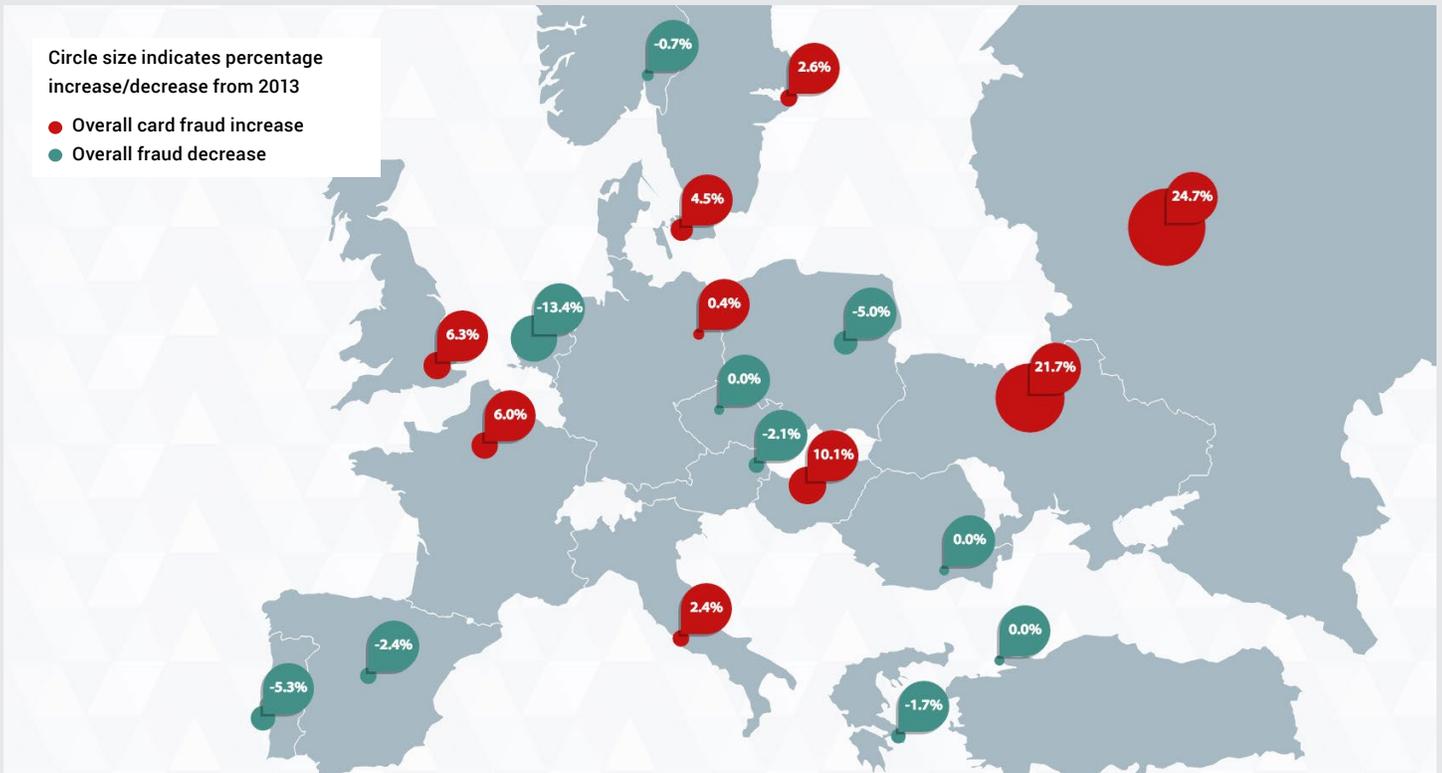
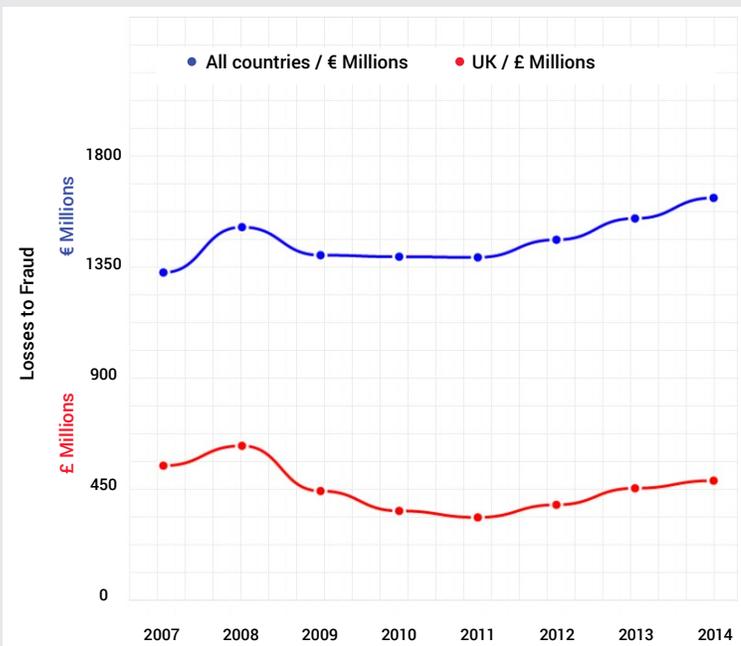


Figure 2: European Fraud Map 2014



Data provided by Euromonitor International

## Card-Not-Present Fraud

### Remains the Biggest Threat

Last year saw modest increases in fraud losses from cards issued in Europe, as shown in Figure 2. The countries with the highest fraud as measured in basis points (1/100th of a percentage of card sales) have not changed from what we reported last year. As shown in Figures 3 and 4 on the next page, during that same period, however, there was a slight increase in basis points for many countries.

Figure 3: Fraud Severity Levels 2014

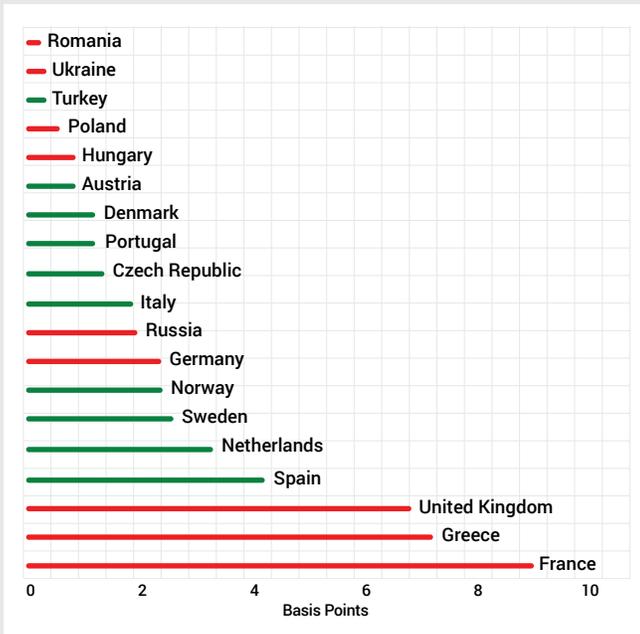
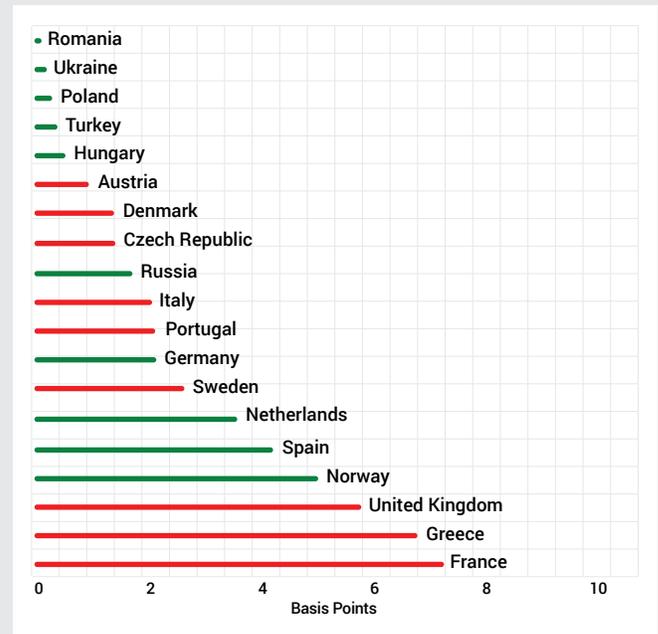


Figure 4: Fraud Severity Levels 2013



Red lines indicate countries where the card fraud rose from 2013 to 2014, green lines where it decreased.

### Are We Winning the Fight Against CNP Fraud?

As FICO has reported for the last three years with its European Fraud Map, a major challenge today is card-not-present (CNP) fraud. The primary threat from a decade ago, counterfeit cards, today represents just 10% of the total plastic card fraud mix in the UK, and that is similar across many European countries.

So, are we winning the fight against CNP fraud? Using the UK market as an example, the answer is a cautious yes. CNP fraud back in 1998 represented just 10% of the total card fraud losses, but by 2008 – the last peak in UK and European card fraud – the losses had grown to 24 times the 1998 figure and represented 54% of the total fraud losses. In 2014, CNP fraud represented 70% of the total losses. However, the losses in the UK stand at only £3 million more than in 2008.

If you look at these numbers in the context of the changes in spending over this period, you start to see that UK banks and retailers have made real gains. EMV had rolled out by 2006 and fraud was migrating as expected to CNP and cross-border fraud. E-commerce spend in the UK in 2007 was £41 billion – it had more than doubled by 2013, reaching £91 billion.

The rise in online spending alone would have attracted criminals, and if CNP fraud losses had grown at the same rate as CNP spending, we would have expected UK CNP losses to be more than double 2008's figure of £328 million – instead, in 2014 it was just £3 million higher at £331 million, an increase of less than 1%.

## Devices and Dynamic Authentication

We may be winning the fight against CNP fraud, but we still have a long way to go to get it fully under control. Authentication of customers and their devices will play an ever-increasing role.

Customers are targeted because they have the data that criminals want to commit fraud. And people have more devices than ever that can open the door for criminals.

In the UK alone, 11 million internet-enabled devices were received as gifts at Christmas in 2013. Only 44% of those people will implement internet security on those devices, and less than one in three will use complex passwords to protect the devices. What's more, 57% of people in the UK do not even check that a web site is secure before making a purchase. It should not then be surprising that we have so much media attention around cybercrime, and that malware attacks are becoming more and more sophisticated.

Being dynamic in authentication of customers will be a great boon, because theft of data will have less value to criminals. Good authentication, such as two-factor using cryptograms, exists in the online banking world and that's why it represents just 12% of the UK card fraud losses. Changing EU regulation, such as the new SecuRe Pay mandate, is also bringing authentication and identify assurance to the fore. In conjunction with industry initiatives such as tokenization, FICO's advances in analytics that assess consumer behavior, and profile not just cardholders but devices and merchants, will help the industry win the war against fraud across Europe — and beyond.

## The Impact of EMV Adoption in the US

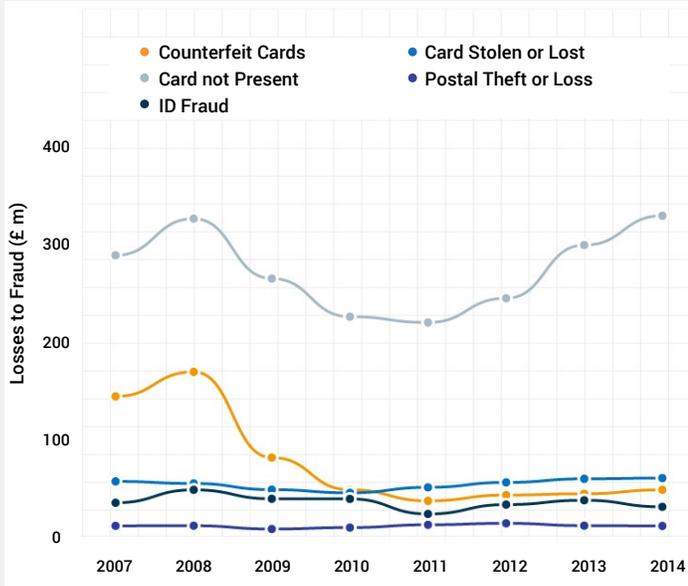
The US is moving toward the EMV liability shift in October 2015 for Point Of Sale, followed by ATM and unmanned petrol terminals in 2017. The US has seen an **unprecedented increase in attacks on ATMs** through skimming on both bank-owned and non-bank estate ATMs. This implies that criminals are making the most of mag stripe technology fraud before it becomes far more difficult to get away with it in the US.

In the UK, FICO has identified a **25% increase in cross-border fraud on debit cards in 2014**, compared to 2013. More importantly, it identified that 47% of the fraudulent transactions were taking place in the US — a pattern that, again, seems related to the delay in EMV adoption in the US.

Given that most European banks shut their doors against mag-stripe fraud years ago, it may appear that they have little to worry about. However, these trends suggest that any European plastic card is also being targeted, as criminals try to "fill their boots" before the US finally shuts the door on skimming fraud.

## Spotlight: United Kingdom

### Cross-Border Vulnerabilities Drive UK Losses



Data provided by Euromonitor International

UK card fraud losses rose by £29 million in 2014, a 6% rise on the previous year. However, when you look closer at the losses, you see that the loss increase was directly related to cross-border fraud. Domestic losses remained at the same level as the previous year, with small reductions in ID theft being replaced by domestic CNP fraud.

Fraud migration, the trend we've illustrated for the past few years with the European Fraud Map, is alive and well — only now it's global. It looks like UK cards are getting caught up in the rush of criminals seeking to exploit the slow adoption of EMV in the US, and we believe the same is true for other European cards, as counterfeit (skimming) continues to find a country with mag-stripe technology. And, of course, even after the liability-shift dates there will be the "actual" implementation timeframes that will determine when these defences are fortified.

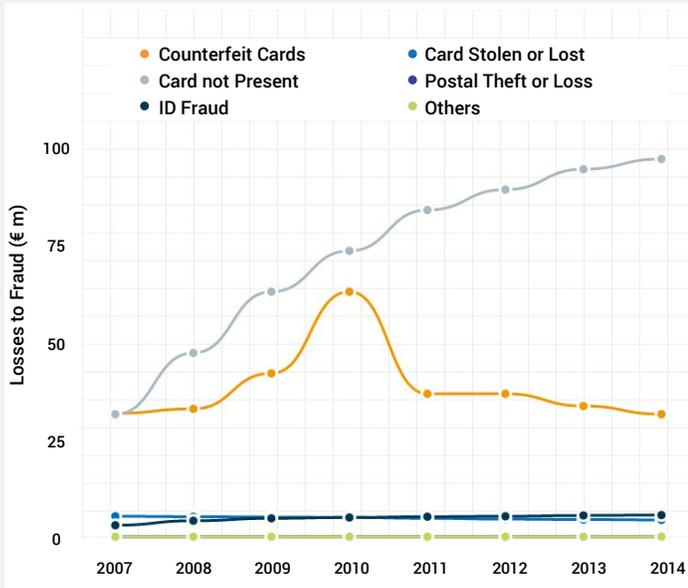
CNP fraud is the other big story revealed by the data analysis, with counterfeit, lost and stolen and intercept fraud (theft of card from postal system) flat. Still, that has not stopped criminals trying to compromise cards and PINs, by calling targeted vulnerable people and purporting to be their bank or even the police.

With CNP at 70% of total card fraud losses and continued growth in genuine e-commerce spending, combined with the directive to keep customer experience at the top of the priority list, all efforts are focused on managing fraud without upsetting customers. Getting that customer experience right will deliver benefits — Gallup recently reported that fully engaged customers yield 23% more in terms of share of wallet than the average cardholder, while disengaged cardholders deliver 13% less.

Fraud has become one of the decisive moments for cardholders. Many banks are getting better at managing fraud and are ensuring that they contact the customer in real time using technology such as FICO® Fraud Resolution Manager, which is widely used in the UK and other global markets.

## Spotlight: Germany

### CNP Fraud Jumps as Counterfeit Falls



Data provided by Euromonitor International

Counterfeit and CNP fraud are the dominant fraud types in Germany and account for 93% of the total card fraud losses. Overall, the plastic card fraud losses have been stable and the slight reduction in counterfeit has been offset by a sharp increase in CNP losses.

Earlier this year, FICO reported that **credit card fraud in Germany increased by 17% over the previous year**, and comparing this to normal sales growth of 5% you can see that criminals are continuing to apply pressure. Fraud losses as a ratio of total credit card sales are running at 11 basis points. However, the figure for overall card losses is just 2 basis points, which reflects the fact that debit cards are the dominant card in use in Germany, and fraud losses on domestic use of these cards is low.

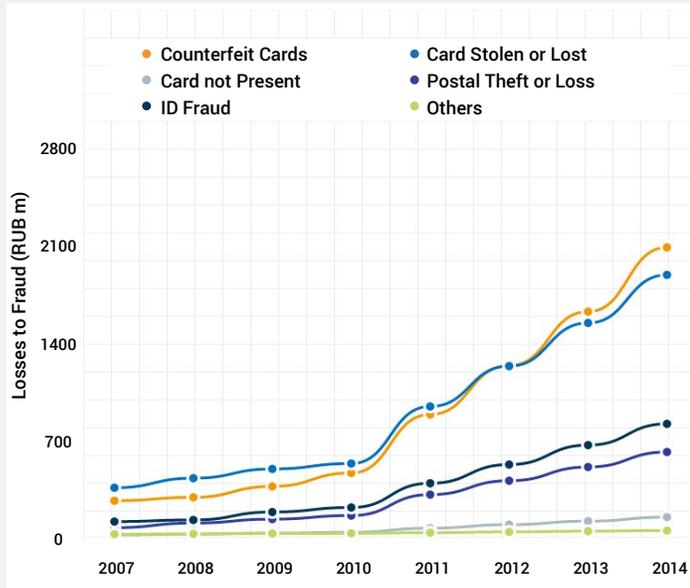
We also observed that 70% of the fraud in our earlier credit card sample was CNP, with 23% counterfeit, indicating that card compromise is at the top of list for criminals. Added to that, criminals carry out 80% of the credit card fraud cross-border, which fits with the trends experienced in the UK and cross-border growth generally.

(Criminals also stand a lower risk of being caught by the police outside German borders than within. Preventing and prosecuting criminals cross-border requires effective cooperation between criminal justice officials in different jurisdictions.)

Having such a high percentage of cross-border fraud brings its own challenges in terms of customer experience when people are traveling or taking their hard-earned vacation this summer. Having good controls and customer communications capability will be the key to managing cross-border fraud attacks and allowing those on holiday to spend when and where they want.

## Spotlight: Russia

### Old-Fashioned Tactics Fuel Sharp Rise



Data provided by Euromonitor International

Russia continues its high growth trend for another year, with fraud losses growing 24% over 2013, which in turn had recorded 28% growth vs. 2012. The actual growth amount in 2014 is 2.5 times the amount of losses recorded back in 2006, and the growth in counterfeit losses is the highest at 29%, which is different to more mature markets for plastic cards, such as the UK and Germany. This growth is not surprising, given that Russia's card spending grew by 36% in terms of monetary value from 2013 to 2014, and by 16% in terms of transactions.

Counterfeit makes up nearly 40% of the total losses and reflects the opportunity afforded the criminals in a country where EMV transactions represent only around half of all "face-to-face" transactions, compared to 96% in Western Europe. Still, growth in EMV transactions did grow by 8% in 2014, so there will be a change to a mix of fraud similar to Western Europe as Russia closes the door on mag-stripe counterfeit fraud.

CNP fraud is running at just 3% of losses, which won't rise until the criminals are forced to change their attack. UK and Germany have CNP at 70% of the total fraud mix, and that's the trend that is expected as Russia completes rollout of EMV in the region.

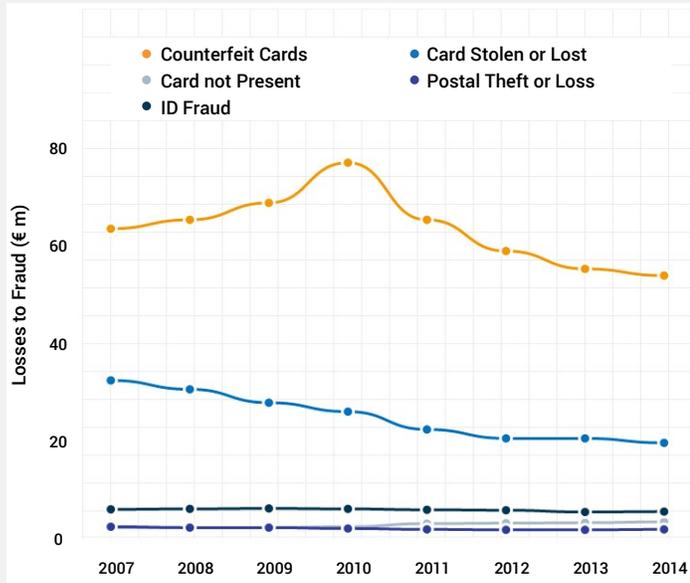
Given that criminals prefer card-present fraud, it's no surprise that lost and stolen is the second highest area of loss, with 33% of the total losses. Lost and stolen is expected to decrease as EMV moves to cover 80% of transactions, because in Russia the PIN will be required as well as the stolen card. It will no longer be viable to steal the wallet or handbag without first observing the PIN being entered at an ATM or POS device.

Theft of cards from the postal system is around 11% of the losses, and, again, this is expected to decrease as EMV adoption increases, because once all of the PINs have been issued to customers then the card is of no use on its own, and as a result is no longer as much of a target.

Any growth market attracts ID theft as criminals try to exploit marketing and the originations process to get a good card and PIN with which to commit fraud. ID theft is around 15% of the total losses in Russia, three times the percentage seen in a mature market such as the UK. Russian issuers should watch out in this area as EMV use grows — criminals need that good card and PIN, and why steal it if the bank will send you one through the post?

## Spotlight: Spain

### Counterfeit Fraud Remains Dominant



Data provided by Euromonitor International

Spain has a very different fraud mix than the rest of Western Europe. You would not expect to see CNP fraud at 4% of the total losses elsewhere.

Counterfeit has always been the dominant fraud type, with 65% of the total losses. Because Spain is located in a mature EMV market for card-present transactions, most of the losses are cross-border; domestic counterfeit within Europe will attract a liability shift, as per scheme regulation, where the weaker technology attracts the loss. So a good EMV card trumps a weaker mag-stripe POS terminal and the retailer suffers the loss. However, this does not apply out of region, so any losses in the US on mag-stripe transactions will remain the issuer's responsibility.

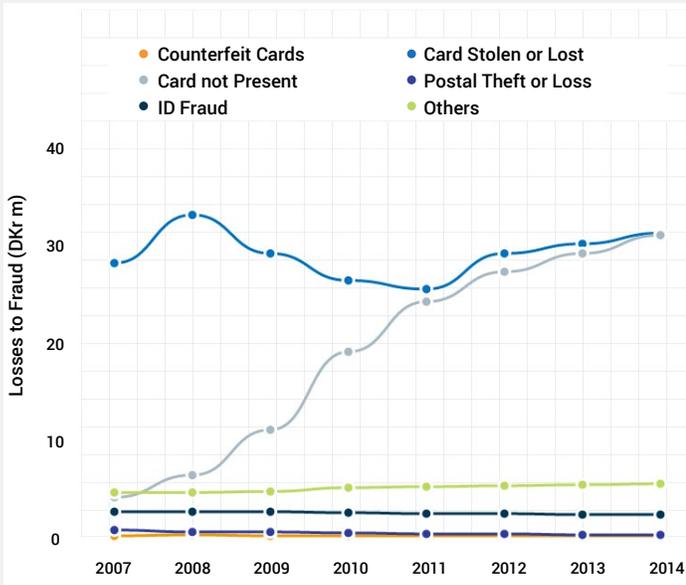
When you have high levels of cross-border counterfeit fraud, you need good fraud detection capability to minimize the impact on customers. The fact that counterfeit only fell by €1.5 million last year suggests that the capability is either not in place, or it is not being used in an aggressive manner.

Lost and stolen is around a quarter of the total losses, so 90% of the total losses are related to counterfeit and lost and stolen, a pattern less like Western Europe than what Russia is currently experiencing. It seems that Spain still has a culture where criminals try to steal the good card and PIN, because this has represented about a quarter of the losses going back to 2007. Strangely enough, in 2006 it represented nearly 60% of the losses, and counterfeit was just 20%. This shows the fluidity of the fraud threat, which constantly morphs to find the weakest link – sharpening analytic detection of fraud is critical to keep losses under control.

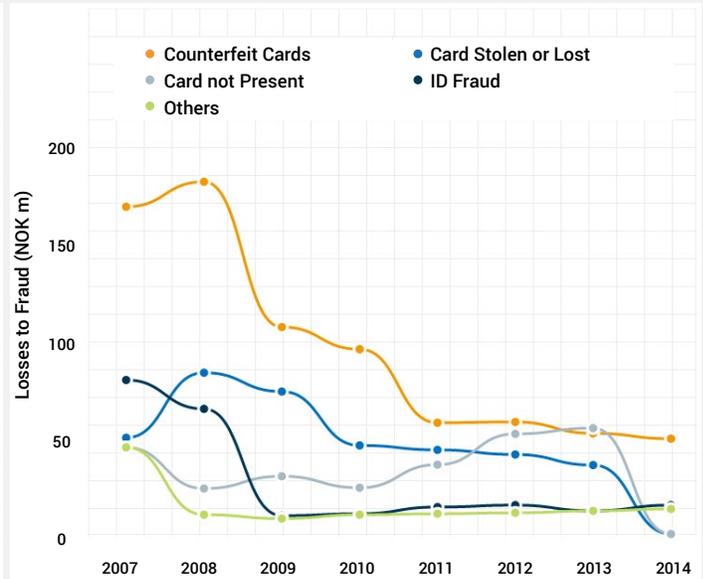
Many years ago, in an attempt to slow counterfeit in the domestic market, Spain added information to the mag-stripe track, which was read and checked by card issuers for transactions at ATMs. It may be that the requirement to obtain (steal) the good card to commit ATM fraud has carried on throughout the EMV rollout, and thus is a legacy fraud problem specific to the Spanish market.

Spotlight: Nordics

Denmark



Norway



Data provided by Euromonitor International

Denmark has far less fraud overall than its Nordic colleagues, with just over a quarter of the losses seen in Sweden. Its losses are made up of lost and stolen, which is now at roughly the same level as it was in 2008, and CNP fraud, which has increased to 50% of the Danish losses.

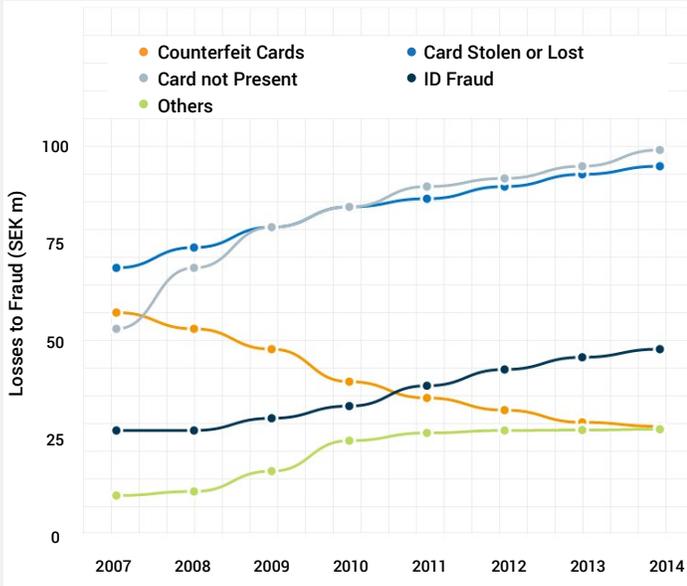
This increase aligns with the adoption of EMV. However, lost and stolen has not reduced at all over the period and it may need review (see also Sweden). Countries such as the UK have reduced lost and stolen fraud because of “challenge teams” that focus on the kind of first-party, opportunistic fraud attacks that should be more evident in the world of EMV protection. Even if this turns out not to be first-party fraud, it’s worth a detailed look so as to find hot spots of theft – these can then be the targets of media campaigns aimed at customer awareness, combined with greater police visibility.

Norway has seen a dramatic reduction in fraud since 2009 – counterfeit fraud alone has fallen by 54%. Counterfeit fraud still represents nearly one-third of total fraud losses, but that is down from representing half of the total fraud losses in 2008. Losses from lost and stolen cards have been halved since 2008, which is also good news for Norwegian issuers.

CNP has increased over the last couple of years, which is to be expected with the growth in e-commerce and internet-enabled devices in Europe. This will continue to be a challenge for Norway and the rest of Europe.

Spotlight: Nordics (continued)

Sweden



Data provided by Euromonitor International

Sweden has also seen a reduction in counterfeit fraud, which is now at half of the amount reported in 2008. However, we have seen an overall increase in fraud – lost and stolen alone is 28% higher than in 2008, which shows that criminals are reverting to the theft of good cards and PINs.

CNP fraud is 44% higher than in 2008, following the trend we see across most of Europe.

What is not expected is the sharp rise in ID theft, which is 80% higher than in 2008. This suggests that criminals have migrated back to theft and deception on the back of the work done to reduce counterfeit fraud.

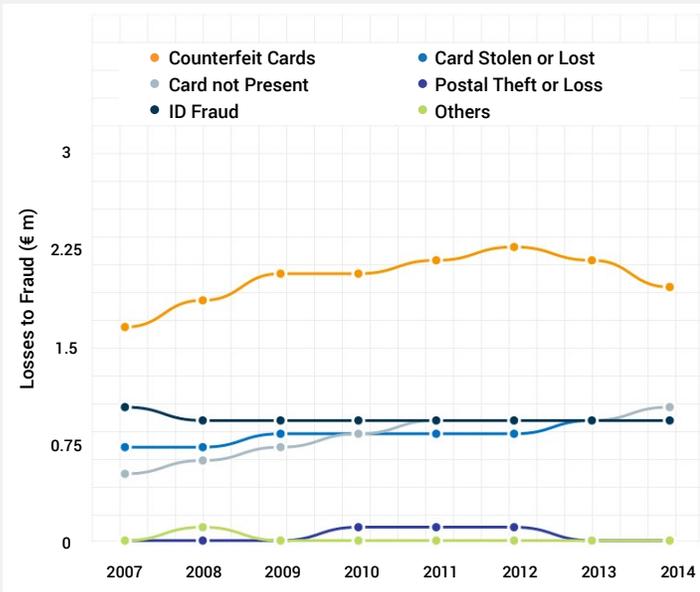
Migration in fraud is always a worry. When you focus all your efforts in one area, as Sweden has done with positive impact on counterfeit, you force criminals to explore other opportunities. Fraud at the point of account origination will surely be exploited if not adequately protected, as shown by the steady increase over the years.

Lost and stolen is another area that needs some attention – issuers need to find the root cause behind the continued increase. This should have reduced since 2008,

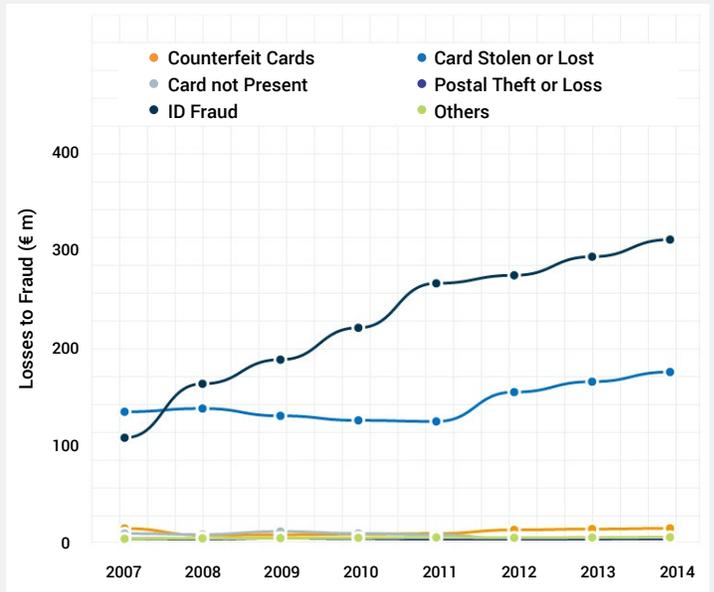
and the fact that it has not suggests that criminals still find the system vulnerable. Some detailed analysis is required to pinpoint hot spots of attack or potential first-party fraud. In the mag-stripe world, first-party fraud can be as high as 15% of total card fraud losses, but in a chip and PIN environment it's far harder to get away with because your card and PIN need to be compromised. As noted in the commentary on Norway, this is worth a detailed look and perhaps the creation of a "challenge team" to focus on reducing the losses.

## Western Europe

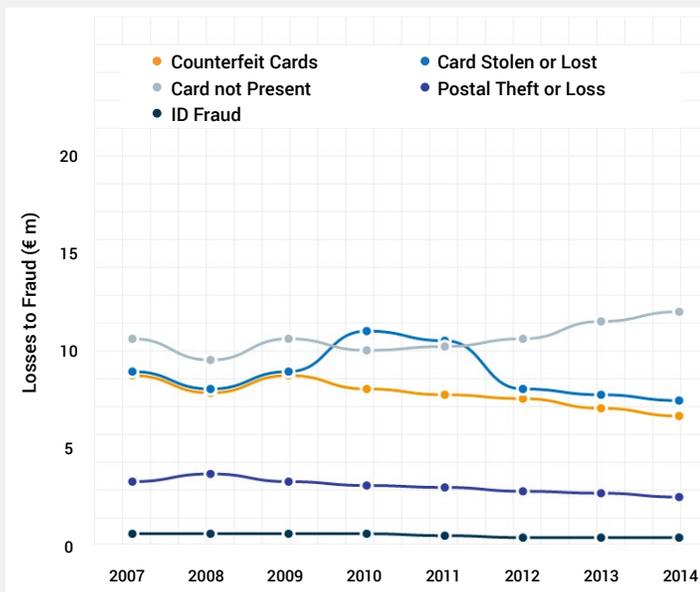
### Austria



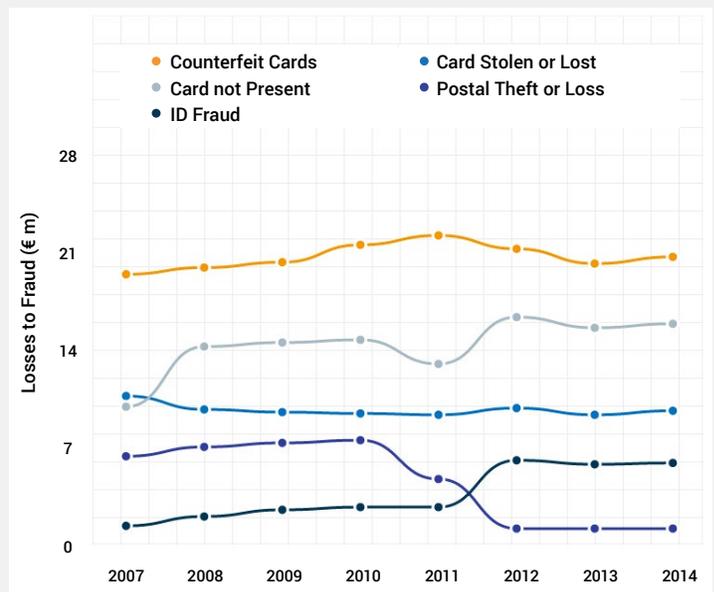
### France



### Greece

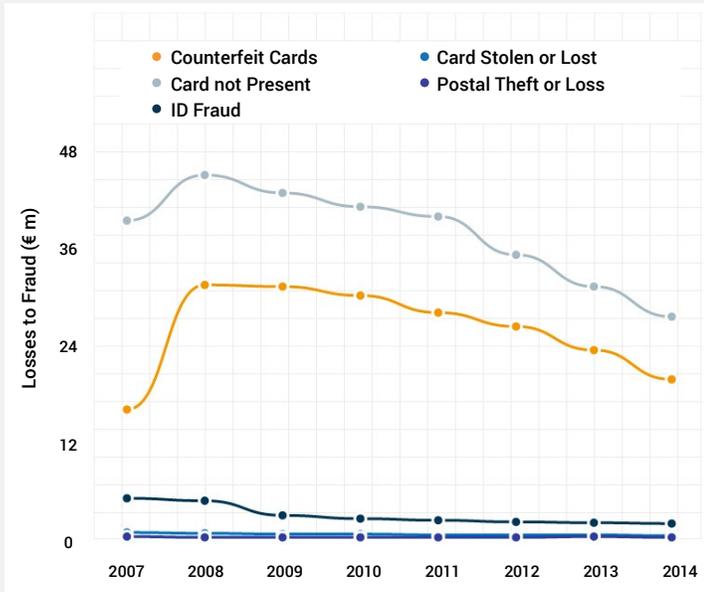


### Italy

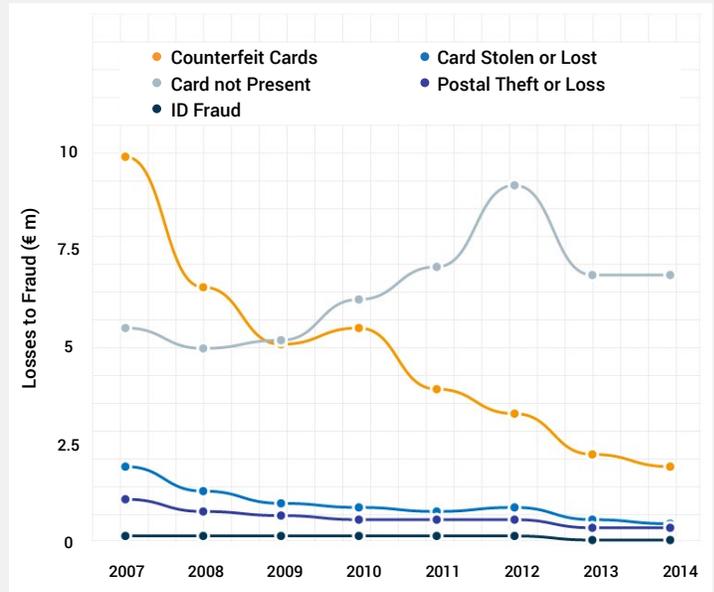


Data provided by Euromonitor International

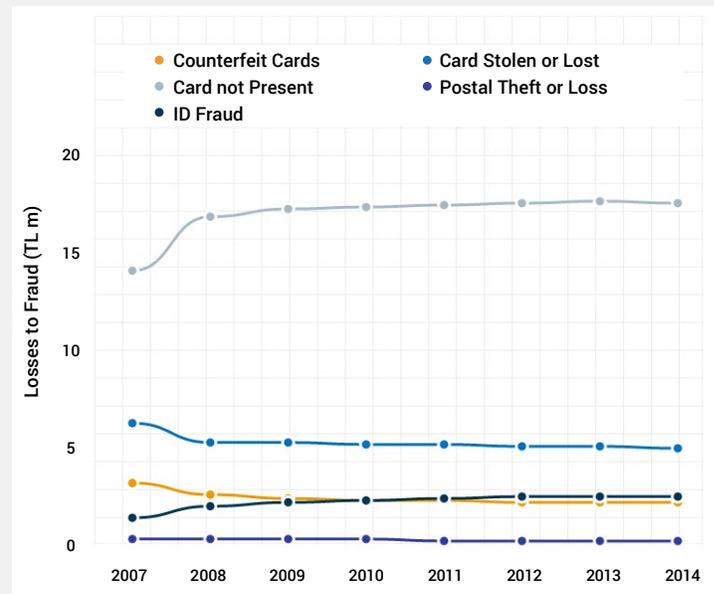
Netherlands



Portugal



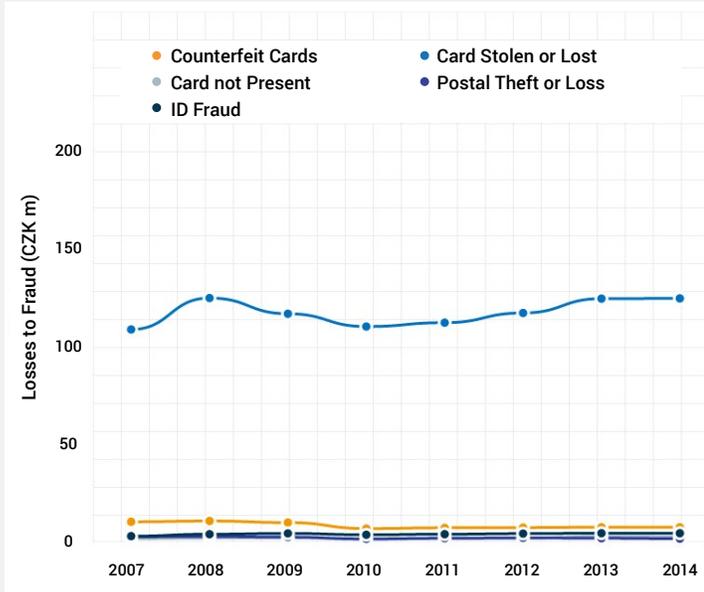
Turkey



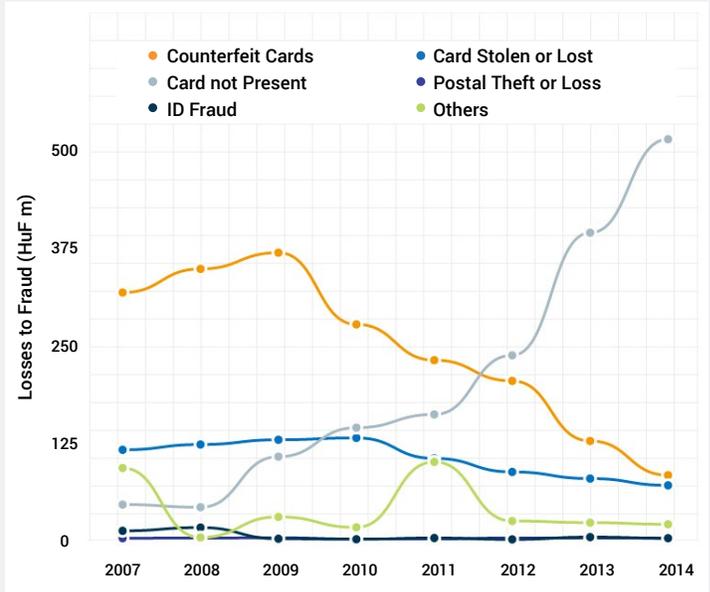
Data provided by Euromonitor International

## Eastern Europe

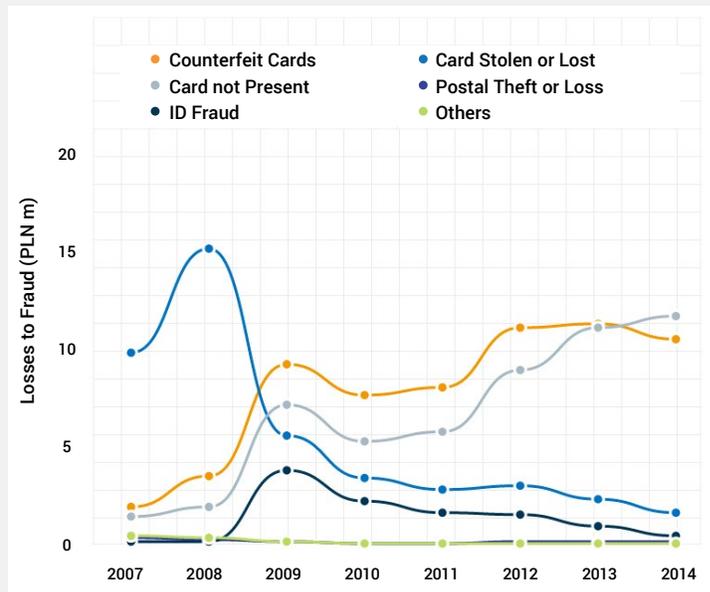
### Czech Republic



### Hungary

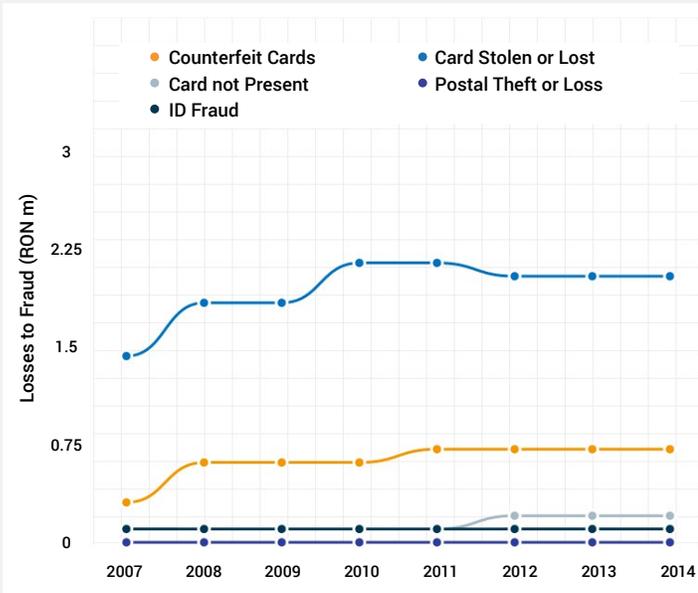


### Poland

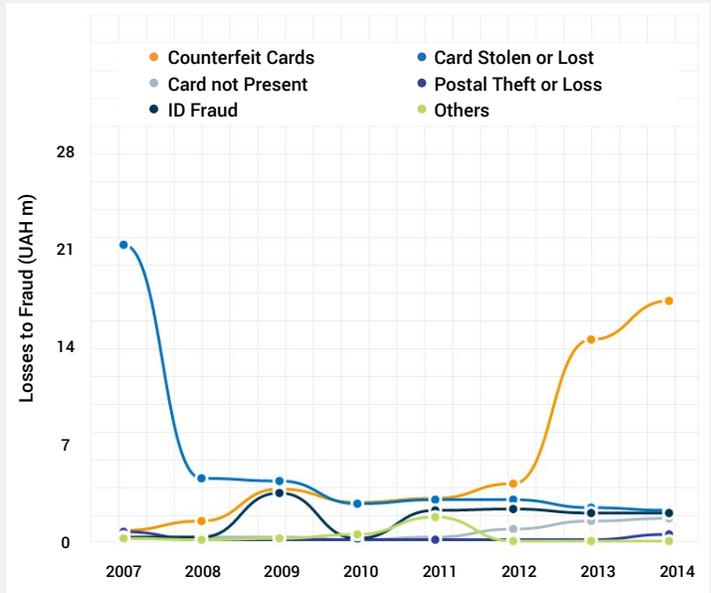


Data provided by Euromonitor International

Romania



Ukraine



Data provided by Euromonitor International

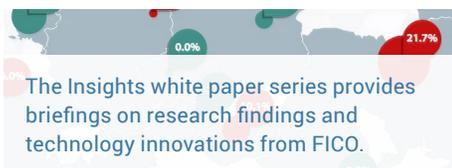
Conclusion

Adoption of EMV continues to shift the fraud types across Europe, but fraud remains a problem that needs to be aggressively managed. As the US adopts EMV beginning this year, the patterns around the world are likely to change. It has never been more important for issuers to adopt the latest analytic advances and best practices in their fight against criminals.



To learn more about best practices in fraud management, visit the FICO [fraud microsite](#) and [fraud blog](#), and read these Insights white papers, all available on [FICO.com](#):

- Fraud: Customer Experience Breaker or Maker?
- Is It Fraud? Or New Behavior?
- Can Fraud Alerts Raise Customer Loyalty?
- Best Practices for Preventing Data Breaches



FOR MORE INFORMATION  
[www.fico.com](http://www.fico.com)  
[www.fico.com/blog](http://www.fico.com/blog)

NORTH AMERICA  
+1 888 342 6336  
[info@fico.com](mailto:info@fico.com)

LATIN AMERICA & CARIBBEAN  
+55 11 5189 8267  
[LAC\\_info@fico.com](mailto:LAC_info@fico.com)

EUROPE, MIDDLE EAST & AFRICA  
+44 (0) 207 940 8718  
[emeainfo@fico.com](mailto:emeainfo@fico.com)

ASIA PACIFIC  
+65 6422 7700  
[infoasia@fico.com](mailto:infoasia@fico.com)