CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Country Risk Analysis

European Card Fraud – Why Have Card Fraud Levels Hit an All-time High?

Martin Warwick

Martin Warwick
Principal Consultant
FICO

Biography

Martin Warwick is Principal Consultant at FICO (www.fico.com) with specific responsibilities in Fraud Consulting – a position he has held since 2007. Previously Martin headed up the Fraud Operations at Barclaycard with responsibility for over 20 million plastic cards, leading a team of over 400 people. He has over 28 years of plastic card experience with Barclaycard in various roles and responsibilities from fraud through to work study, operations and projects.

Martin was also heavily involved in major industry fraud prevention initiatives such as the roll out of Chip & PIN. Being heavily involved in the fight against fraud in the UK, meant that Martin was invited to sit on many industry bodies such as the UK, European and International Risk Advisors groups for Visa as well as being a member of the Plastic Fraud Prevention Forum at APACS for many years.

Keywords Fraud, European card fraud, CNP fraud, Financial Services, Behavioural analytics, Data
Paper type Research

Abstract

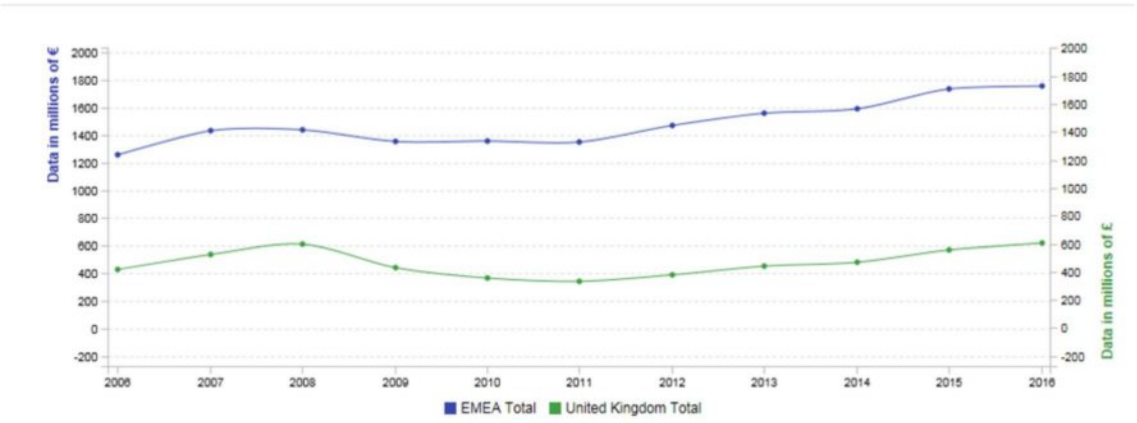
Card fraud is a topic that has rarely been out of the headlines, as companies across Europe face up to the rising number and increasing severity of incidents. FICO's annual study of European card fraud reveals the extent of this problem in recent years. As the author of this article explains, hiding amongst the growth in online purchases is great from a criminal point of view, but for some financial institutions finding and stopping fraudulent transactions is getting tougher.

Introduction

The growth in online spending and CNP fraud brings new challenges for banks and retailers, as criminals thwarted by chip & PIN have moved to a less risky channel. Hiding amongst the growth in online purchases is great from a criminal point of view, but finding and stopping fraudulent transactions just gets tougher. Spotting the 'needle in a haystack' requires new behavioural analytics and artificial intelligence, combined with enhanced information from outside the traditional data contained within a purchase.

FICO's annual study of European card fraud reveals the extent of this problem in recent years. After increasing by 10% in 2015, card fraud levels soared to a record high of €1.8 billion in 2016. Card not present (CNP) fraud has persisted as the fraud type that generates the highest losses: comprising 50% of gross fraud losses in 2008, it grew to 70% last year, driven by a surge in e-commerce transactions.

Figure 1: Total fraud levels



Source: FICO European Fraud Map – www.fico.com/europeanfraud

These figures, based on a survey of 19 European countries, contain some important lessons for financial institutions looking to fight fraud.

Lesson one: Criminals are constantly adapting

From a regional perspective, CNP fraud dominates the overall fraud landscape in Europe. This trend stems from the fact that the major European financial hubs, such as Germany and the UK, are also strong centres of e-commerce. In other countries however, historical factors have created entirely different patterns of fraud. Criminals follow the line of least resistance, and being able to hide in a huge growth channel is perfect for their needs.

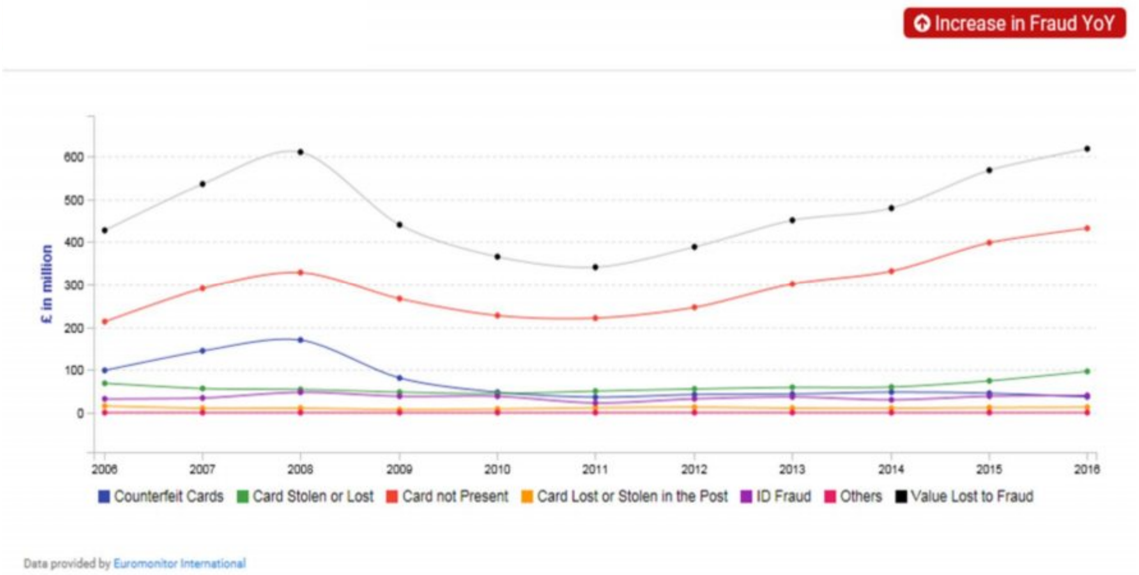
With a large and growing stream of card transactions, it is not surprising that the UK has been particularly hard hit, topping the list of countries for the highest card fraud losses in 2015-2016. In 2015, the UK contributed a staggering 44% of the total registered losses across the 19 countries surveyed. In 2016, losses amounted to £618 million, or 43% of the total losses in Europe.

Not only was the amount lost in the UK in 2016 a 9% rise over 2015, but it also topped the previous peak in card fraud, set in 2008 before the adoption of a 'tough on fraud' stance that introduced the use of chip and PIN. These results coincided with the spike in domestic e-commerce spending: figures from Financial Fraud Action UK reveal that genuine online spend was £41 billion in 2008, and £248 billion in 2016 – a six-fold increase in just eight years.

This exponential surge in e-commerce transactions has re-emboldened criminals to target this area. Although CNP fraud was pushed down to £220 million in 2011 from £328 million in 2008, it rose again to hit £432 million in 2016, with e-commerce representing a substantial chunk at £309 million.

It has even been estimated that UK consumers will use their mobile devices to manage their current accounts around 2.3 billion times — that's more than traditional branch banking, telephone banking and internet banking combined. With the popularity of e-commerce showing no signs of abating, it is likely that CNP fraud will continue to be the main channel of revenue for fraudsters for the foreseeable future.

Figure 2: United Kingdom



Source: FICO European Fraud Map – www.fico.com/europeanfraud

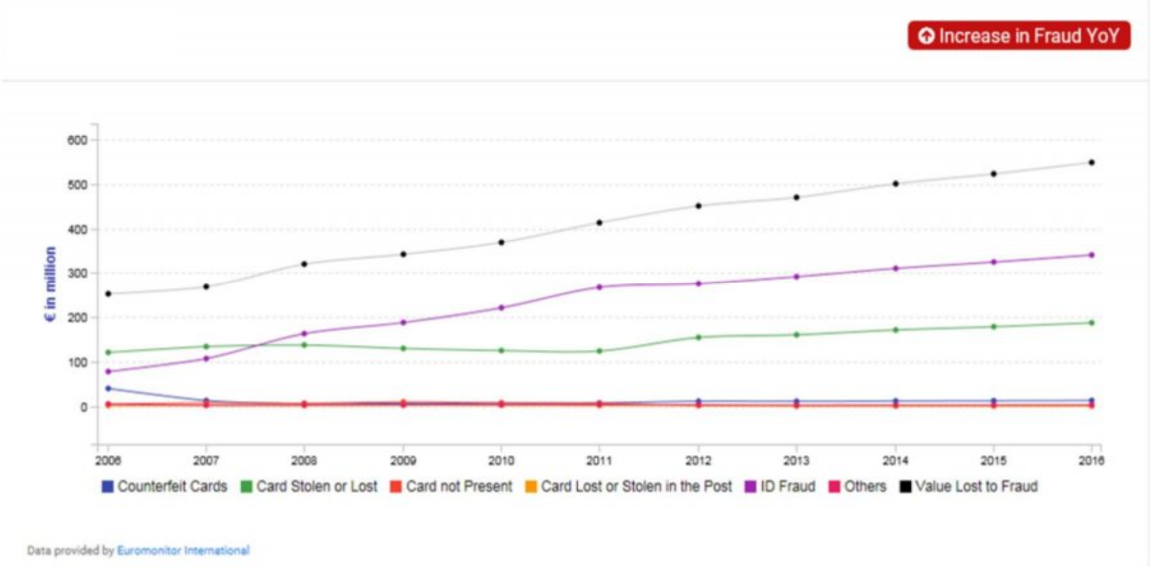
At the same time, be wary – card fraud trends across Europe can vary from country-to-country. Take France, which ranked in the top five countries for fraud losses in 2015-2016, where ID Fraud and Lost & Stolen (L&S) fraud accounted for 96 per cent of the total losses in 2016. In Spain, a country with one of the highest fraud-to-sales ratios, CNP fraud has yet to even register; Counterfeit fraud leads the pack instead.

These discrepancies have been built on historical foundations.

France introduced chip and PIN payments to secure its point of sale systems 12 years ahead of Europe and the rest of the world; an investment that ensured it enjoyed a low level of Counterfeit fraud compared to the rest of Europe in the early 2000s.

To circumvent this obstacle, criminals realized that they needed to steal the card and associated PIN from the consumer, apply to banks for credit using false identities, or actually take over a customer's account at the bank. As a result, ID Fraud constituted almost two-thirds of the country's 2016 fraud losses.

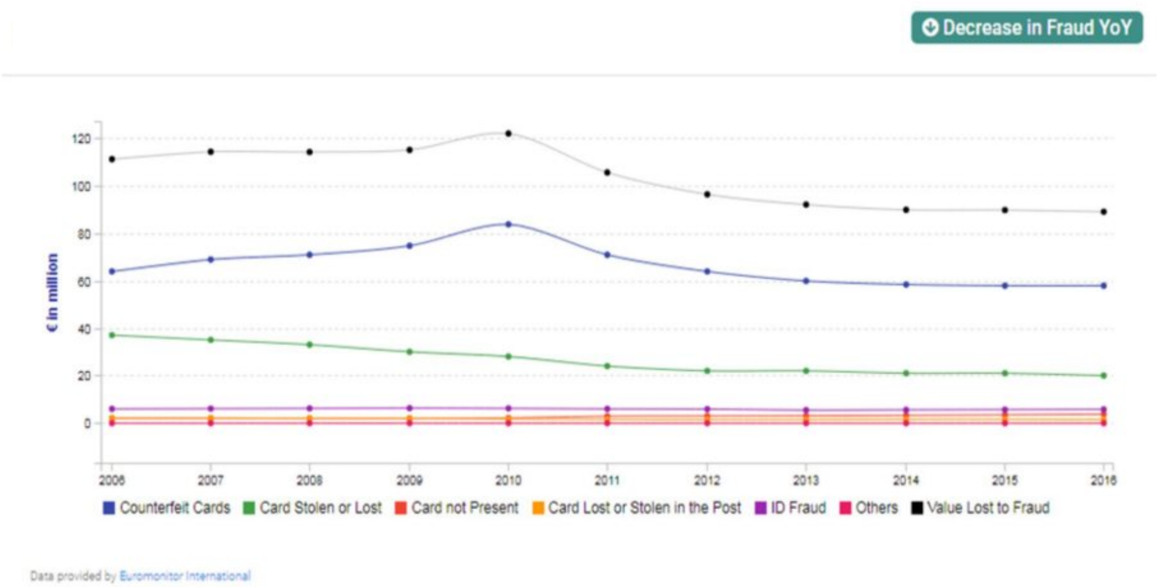
Figure 3: France



Source: FICO European Fraud Map – www.fico.com/europeanfraud

In contrast, Spain was slower in the roll-out of chip and PIN, which encouraged criminals to continue focusing on Counterfeit fraud in cross-border transactions. Naturally, this became the dominant fraud type, comprising 62% of Spain's total card fraud losses in 2016.

Figure 4: Spain



Source: FICO European Fraud Map – www.fico.com/europeanfraud

Going forward however, we cannot expect the dominant types of card fraud in each country to remain the same. Criminals are constantly adapting to the latest fraud prevention technologies, and will seek to exploit fresh weaknesses.

Returning to France, we would soon expect changes to the country's fraud landscape, given that French issuers are strengthening their originations capabilities. Thwarted criminals will have to shift tactics again, possibly by returning to e-commerce, meaning a future rise in CNP fraud.

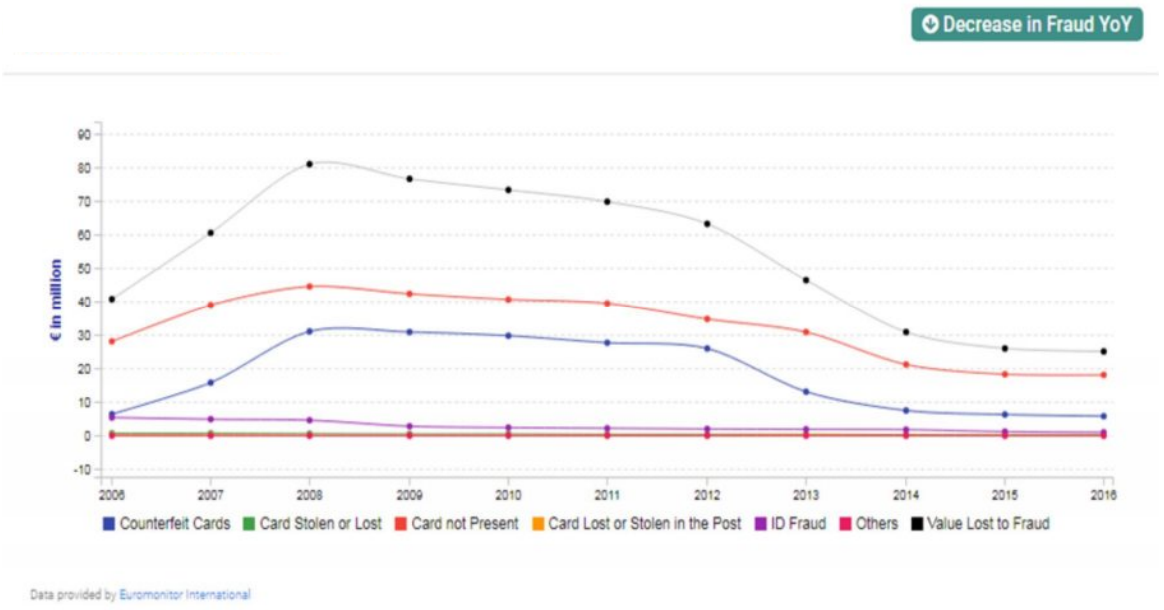
Shifting trends in Russia capture the speed at which criminals move to capitalize on new opportunities. Although losses have been split quite evenly between L&S, Counterfeit and ID Fraud, Russian banks have recently stepped up measures against L&S and Counterfeit fraud. These efforts are reflected in the country's 2016 figures, which show a sharp upswing of 28.5% in ID Fraud, compared to a reduction in L&S fraud, and little change in Counterfeit fraud.

Lesson two: Fraud reduction is achievable and sustainable

The future of card fraud is not all doom and gloom – developments in the Netherlands and Turkey show that, with consistent investment in fraud detection and prevention, it is possible to fight back.

The Netherlands is an example of the gains that sound, strategic investments can reap. Good investment and control decisions deployed by Dutch banks have helped to reduce card fraud by 70% since its 2008 peak.

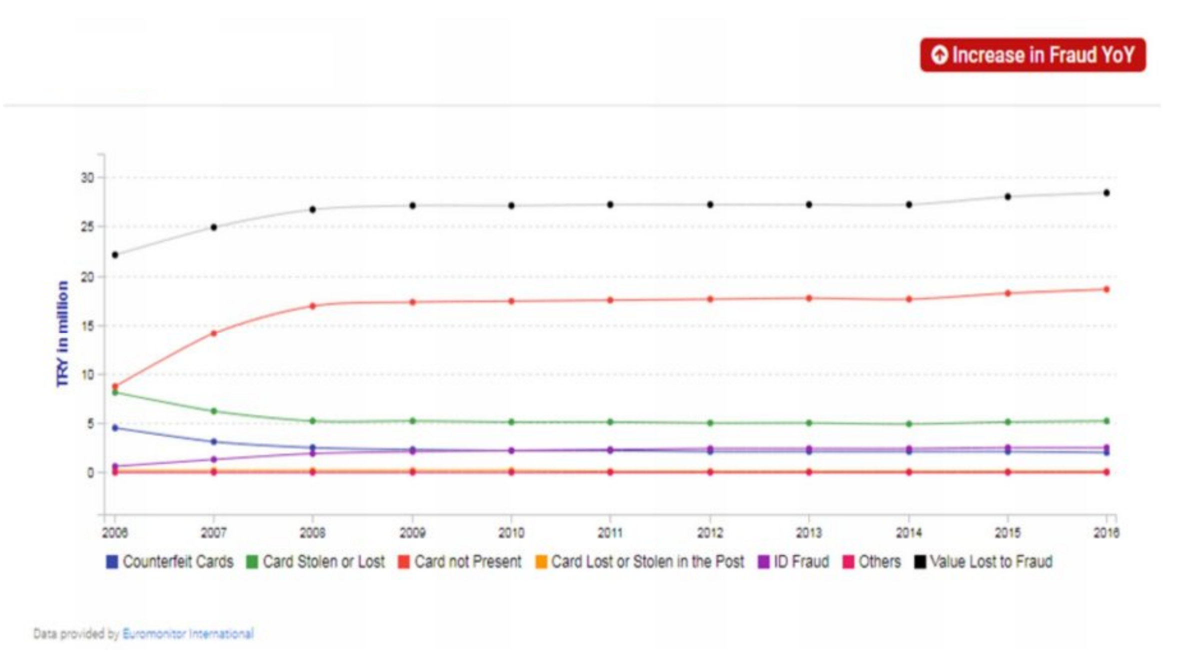
Figure 5: The Netherlands



Source: FICO European Fraud Map – www.fico.com/europeanfraud

In addition, thanks to the dedicated work by its major banks, Turkey has always had a good grip on fraud control. Despite consistently low fraud levels, they have continued to invest in anti-fraud capabilities, which have been largely successful in keeping criminals at bay – the country's fraud levels have risen only slightly to €28.4 million last year from €22.1 million in 2006.

Figure 6: Turkey



Source: FICO European Fraud Map – www.fico.com/europeanfraud

We must however be careful not to overstate Turkey's success. While its banks have undoubtedly made the appropriate investments to keep fraud down, their efforts will go to waste the moment they slacken in this regard. Financial institutions are locked in an endless technological arms race with the fraudsters, and standing still at any moment will hand the advantage over to them.

In order to remedy the current situation – where card fraud levels have risen in 10 out of the 19 countries surveyed in both 2015 and 2016 – there is an urgent need for financial institutions to adopt more advanced anti-fraud solutions.

Lesson three: Fight back with AI

In recent years, many banks have increased their use of dynamic authentication, which validates a user's authenticity with one-time passwords sent to a mobile device, or via biometrics like fingerprint, voice or face recognition.

Nonetheless, the overall figures show it is clearly time for new measures to address these challenges. Developments in machine learning and artificial intelligence (AI) can provide the tools needed to identify fraud faster without compromising the customer experience.

Data volumes are continuing to grow, meaning that analysts are increasingly struggling to sift through all the available information. As more cases become flagged for suspicious activity, so too do the number of false positives. Furthermore, the most prevalent authentication systems are 'high-friction' methods that risk irritating the customer.

This is where behavioural and mobile analytics can step in. A sophisticated solution could tap into the rich source of mobile contexts, such as advanced geolocation and individualized historical transaction activity, and feed it into an effective real-time decision that also has a low customer impact. This approach is a great alternative that provides an extra layer of security when the phone can't be used directly for real-time authentication, or where biometrics might have been falsified.

Behavioural analytics are another mature technology in fraud prevention. It measures consumer behaviour in both the context of their own history, as well as the history of their associated group behaviours. In this way, potentially fraudulent transactions can be flagged with pinpoint accuracy, reducing the volume of false positives. Not only will there be fewer declines on legitimate transactions, but more illicit transactions can be stopped as they occur, potentially avoiding financial and reputational losses.

My colleague Scott Zoldi, FICO's chief analytics officer, explains: "It's no longer just about identifying patterns that are unusual for the customer — we're also looking at anomalies at the mobile device, IP address and merchant level. All of these have 'behaviours' just as individuals do."

Perhaps the most important lesson is that, no matter how low a country's fraud losses are, there is never a case for being complacent. Criminals will seek to exploit every chink in the armour that they can find. Financial institutions should leverage the latest in artificial intelligence-based technologies as part of a sophisticated fraud prevention strategy while maintaining a seamless, 'low-friction' customer experience. This is not an easy balance to strike. But as fraud risks and customer expectations continue to rise, AI-based solutions provide an important path forward for banks.

Reference

Full details of FICO's interactive *FICO European Fraud Map* can be found at www.fico.com/europeanfraud