EMV in a CNP World

Introduction

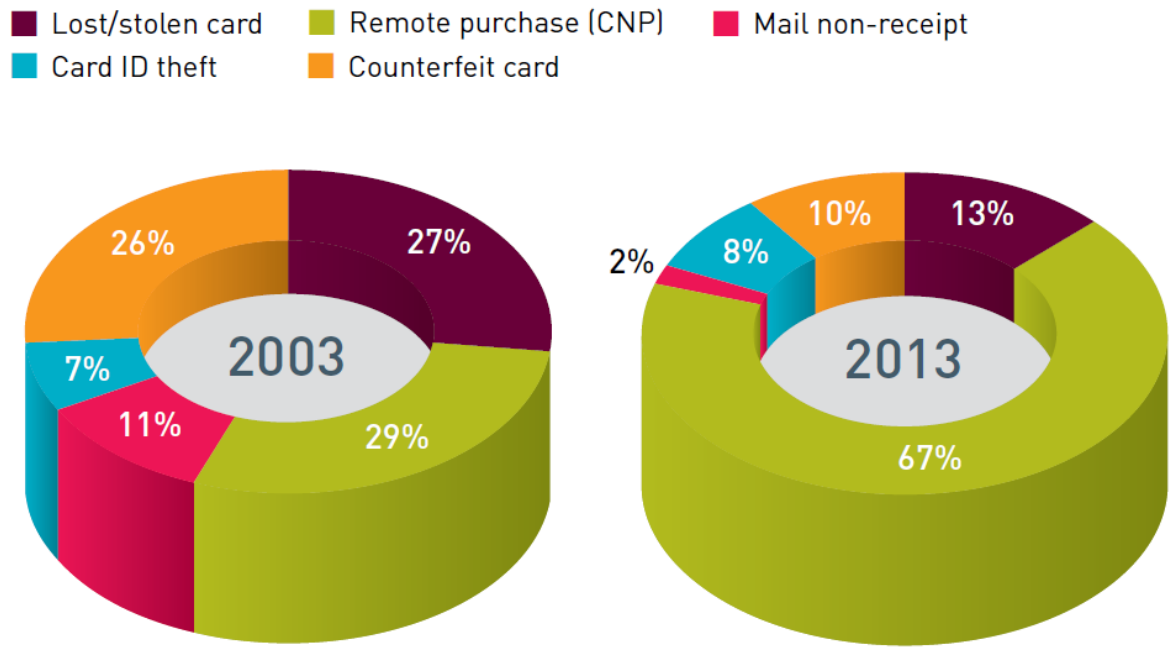
This paper considers the impact of EMV on payment card fraud taking evidence from established EMV markets, mainly focusing on the UK. It will also discuss the impact that the introduction of EMV has had on card-not-present (CNP) fraud, and the steps that have been taken to help manage the risks associated with CNP fraud.

The history of EMV

The concept of Chip payments were first introduced in France in 1984 and saw wider European adoption through the 1990s. The EMV as we know it today was created in 1994 when Europay, MasterCard and Visa together developed the Global EMV standard[1]. The UK began its transition to EMV in 2004. Traction was finally achieved in 2006, and EMV with Chip and Pin became the defacto card acceptance mechanism for face to face transactions.

EMV on the high street

Since the introduction of EMV, face to face fraud losses dropped significantly. Whilst many reports suggest that face to face fraud is non-existent, that would be overstating the point, however reductions in face to fraud have been significant in all EMV countries. The diagram below[2] illustrates the breakdown of fraud types before EMV was launched in the UK, and 2013 by which time EMV had become the norm.



[1] http://blog.elementps.com/element_payment_solutions/emv/
[2] http://www.financialfraudaction.org.uk/download.asp?file=2796

Face to face fraud reduction has been seen wherever EMV has been introduced. Most forms of face to face fraud, from counterfeit cards to lost/stolen and card ID theft benefited from EMV for the simple reason that the card on its own became less valuable for purchasing goods on the high street, unless the PIN was also available to the perpetrator. In addition, merchants generally do not have access to EMV data taken during the payment process, and no longer have the opportunity to obtain magnetic stripe data which is relatively trivial to replicate during a normal transaction. Between 2008 and 2010, the UK experienced a fraud reduction of 45% despite increasing transaction volumes[3].

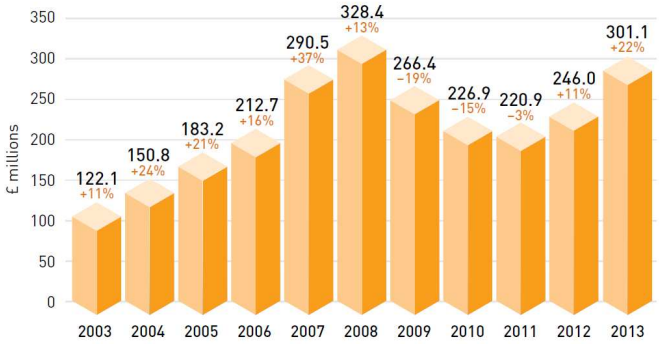
There are a number of factors that have impacted the success of EMV in achieving more in the counterfeit cards market particularly, since although a counterfeit card could not be used in the UK or other EMV countries, the non-EMV market was (un)fair game to the fraudsters. A global adoption of EMV would have a significant impact on reducing the impact of counterfeit card fraud in all parts of the World. This is worth noting, since the US market has suffered as a result of EMV in Europe potentially having been in receipt of these counterfeit cards.

EMV is generally regarded by those regions that have adopted it to date and the single biggest contributor in the fight against face to face fraud and its impact cannot be underestimated. But with that success came a dark side.

The CNP problem

Before EMV, fraud was rife on the high street. It was relatively easy to clone a card, and stealing a card was a quick payday before EMV. Compared to today, there were relatively few controls in place to mitigate against this type of fraud.

Following the introduction of EMV and the added complexity that bought for any would-be fraudster, face to face channels began to lose their appeal. Instead they turned their attention away from face to face channels and towards online and telephone based payments. Statistics document increasing fraud against CNP channels as EMV becomes adopted on the high street. The following table shows a stark increase in fraud levels against CNP channels in 2007, preceded by smaller levels of change in the early adoption phase of EMV in the UK. To help put this into perspective, in 2012, CNP accounted for 63 percent of total card fraud losses in the UK[4].



[3] EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions, Dom Morea, First Data Corporation, 2011

[4] http://www.tsys.com/Downloads/upload/2013_TSYS_EMV_3D_Secure_Report_PC_Video_FinalV1.pdf

EMV was primarily designed as a face to face tool but that doesn't mean that it can't be useful in combatting CNP fraud too. Further, where EMV fails in CNP channels, other fraud reduction mechanisms are in place to help mitigate the losses associated with CNP fraud.

Combatting CNP fraud today

In the UK, CNP fraud has been on the rise, and is around four times that of card present fraud[5]. The payments industry have taken significant steps to reduce the risk of cross-channel fraud. The introduction of EMV in the face to face channel results in reduced opportunity for fraudulent transactions resulting from cards captured in a face to face transaction as merchants generally have no access to EMV data and as such perpetuating cross channel fraud is significantly reduced.

A number of countermeasures have been introduced to help manage the CNP threat. The introduction of 3D secure in 2008 has had some notable success in combatting fraud in ecommerce transactions. When 3D secure was first introduced shoppers often abandoned shopping carts because of the perceived hassle of completing the 3D secure process. Now, 3D secure has moved on and is largely invisible to the cardholder taking place seamlessly within the checkout process, with the exception of some higher risk [*for fraud*] purchases. To quote Visa Europe, "*the fraud rates of transactions that are protected by Verified by Visa[6] run at a quarter of the level experienced by traditional unsecure electronic commerce traffic.*"[7]

3D secure has its issues and it is not the same panacea for ecommerce as EMV has been for face to face; the current use of static passwords does leave the solution open for abuse. And, MOTO still remains a potential channel for fraud that to date is not addressed by either EMV or 3D secure.

Other factors have come in to play that have had significant impact on the level of online fraud. The incredible growth of the ecommerce market and the apparent increase in fraud in the years following EMV adoption masks the success that 3D secure has had. While the statistics show a tripling of CNP fraud, the volume of CNP transactions increased ten times[8]. Consumers now access ecommerce sites from a wider range of devices than ever before which introduces a number of risks to their data outside any risks posed by the merchant website or the payment system itself. As more of our data moves into the online world, so do the people who want to steal that data. The rapid cash-out that is conducted in the aftermath of a major (or less major) data breach also accounts for a not insignificant amount of fraud; in 2012, 24 million card details were stolen from online retailer zappos.com, and the media routinely reports large scale breaches each increasing the risk of fraud against affected cardholders.

In the UK, Visa ecommerce merchants are required to authorise all transactions prior to accepting payment from a card. Visa's internal fraud systems allow for rapid identification of any known or suspected fraudulent cards. In addition, merchants benefit from a payment guarantee when they enrol in the Visa 3D secure program (VbV) which creates an online dialogue with the card issuer and allows them to further validate the card and customer. The use of security code in telephone and online transactions does provide some small assurance that the cardholder is present in the CNP

[5] Managing the card not present fraud environment, Visa, February 2014
[6] Verified by Visa is the Visa branded 3D secure solution, also known as VbV. The MasterCard equivalent is known as SecureCode.
[7] Managing the card not present fraud environment, Visa, February 2014
[8] http://www.tsys.com/Downloads/upload/2013_TSYS_EMV_3D_Secure_Report_PC_Video_FinalV1.pdf

environment since the details are not permitted to be retained by merchant systems[9]. Finally an Address Verification Service (AVS) is available to UK merchants, and is again referenced as part of the checkout process to ensure that invoice address details are legitimate and correctly associated with the card presented for payment and thus providing yet another form of validation.

The future of CNP fraud prevention

There is a lot of discussion in the payments industry focused on addressing CNP fraud. Introducing one-time-passwords as part of the checkout process, whether as part of an EMV based solution, or as a number displayed as part of the payment card itself which continuously updates, is one such solution under consideration at the moment. The use of one-time-only passwords would not only help tackle ecommerce related fraud, but could potentially be used to authenticate telephone payments as well. In an increasingly online world, the drive to provide the same innovative protections for mail order is less attractive, and there is less requirement for it whilst volumes of mail order shopping continue to decline.

There is potential for utilizing capabilities within EMV to provide better security for CNP transactions, and whilst it is not yet commonplace for ecommerce sites, many Internet banks already use its functionality to provide one-time-passwords for web authentication. Some UK banks have provided customers with a card reader device into which they insert a payment card and enter their PIN, to be provided with their one-time-code which must then be provided to gain access to online banking services. This process is also used to set up mobile banking apps as part of the customer authentication process.

EMV in a CNP World

EMV has had a very significant impact on fraud volumes affecting face to face payments and has high value to merchants and the wider Global payments industry for that alone. However, EMV is not the only solution that is required to help combat fraud across all payment channels, and it is only in association with appropriate control measures that comprehensive fraud management can be achieved.

Consideration needs to be given to managing the CNP environment, and where possible, in tandem with the EMV roll out in order to mitigate the potential for fraud migration from face to face channels into CNP ones. Solutions exist and have been operating in the European markets to manage CNP fraud, and especially in the ecommerce environment. There are a number of factors to take into account when reviewing fraud data for this channel, due to its rapid rate of growth, the range of consumer systems and devices that are used for online shopping and any inherent weaknesses therein, and the impact of data theft events.

EMV may in future also provide answers to the CNP problem too. There is potential and capability within the EMV system to enable it to do so. And, despite the increase in CNP fraud post EMV implementation, countries that have adopted EMV have seen reductions in overall fraud and the benefits have far outweighed the cost and effort of implementation.

[9] A requirement of PCI DSS, to which all merchants are required to comply

References

http://www.pymnts.com/exclusive-series/2014/the-truths-and-myths-of-emv/#.VD-xP_nF8bM

http://www.gemalto.com/brochures-site/download-site/Documents/documentgating/fin_emv-payments-myths-truths.pdf

https://www.emc.com/collateral/white-papers/card-not-present-fraud-post-emv-env-wp.pdf

http://www.emv-connection.com/wp-content/uploads/2014/01/CNP-WP-012414.pdf

http://www.bankinfosecurity.com/interviews/fiserv-i-2375

https://www.chasepaymentech.com/faq_emv_chip_card_technology.html

http://www.pymnts.com/assets/Shared/Gemalto-EMV-Whitepaper.pdf

http://www.niceactimize.com/index.aspx?page=news603

http://www.smartcardalliance.org/publications-emv-faq/

https://www.europol.europa.eu/iocta/2014/chap-3-4-view1.html

http://www.firstdata.com/downloads/thought-leadership/EMV_US.pdf

http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf

http://www.paymentscardsandmobile.com/european-card-fraud-losses-hit-new-high/

http://www.tsys.com/Downloads/upload/2013_TSYS_EMV_3D_Secure_Report_PC_Video_FinalV1.pdf

http://www.smartcardalliance.org/resources/pdf/CNP-WP-FINAL-022114.pdf

http://www.financialfraudaction.org.uk/download.asp?file=2796

http://www.financialfraudaction.org.uk/download.asp?file=2795