

Credit Cards & EMV

Will EMV standards impact fraud control?



CREDIT CARDS & EMV: WILL EMV STANDARDS IMPACT FRAUD CONTROL?



Credit cards have evolved from magnetic strips to chip-and-pin, chip-and-choice, and chip-and-signature cards. EMV is now the de facto global standard for the chip technology embedded in financial payment cards. In the fourth quarter of 2012, there were 1.62 billion chip cards in use across 80 countries.

But has EMV really been successful in bringing down incidents of fraud? This paper explores these facets by examining the EMV standards, rate of CNP fraud post EMV implementation and the impact.

QUICK CONTEXT

“The chip proves the card is legitimate. The 3 major features of the chip that make it so unique are what helps to combat fraud – the reason EMV exists.”

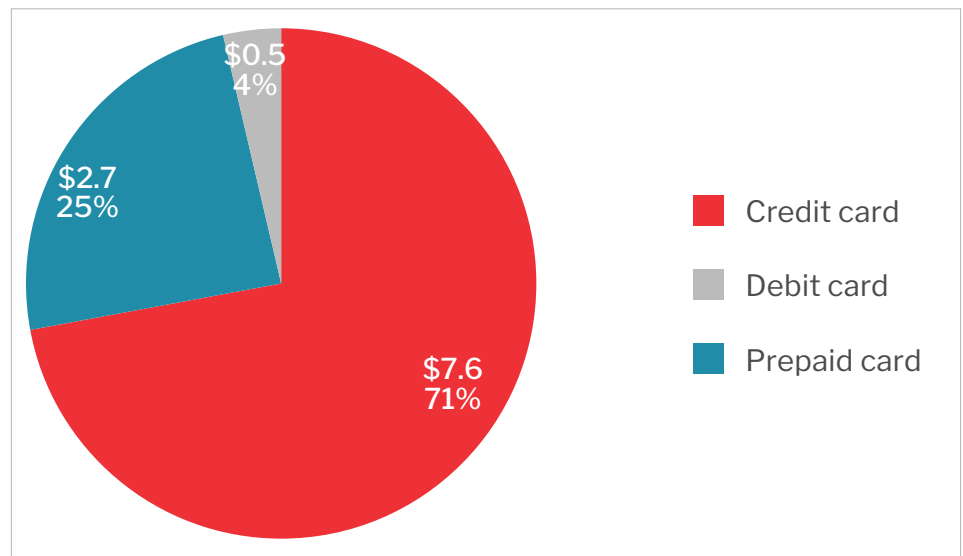
- Mansour Karimzadeh,
CEO, SCIL

EMV (Europay, Mastercard and Visa) is maintained and governed by EMVCo - an independent joint venture of these firms. As opposed to magnetic cards, EMV cards are equipped with micro-computer chips and offer a significantly higher level of data security than stripe cards: data on the chip is secured using both hardware and software security measures, so even if the card data is compromised, the chip itself will still be difficult to counterfeit. The EMV chip carries cardholder and account data and is programmed to make decisions about a transaction and control its outcome, that is, approve or decline it.

EMV cards are fast becoming the global standard for a variety of payment cards including credit cards, debit cards, ATM cards, pre-paid cards, charge cards and such like. Europe, Canada, Latin America and the Asia-Pacific region have already transitioned to chip cards. The United States is the last major country to implement what is now the de facto global standard.

Recent reports reveal that card issuers are losing close to US\$ 11 billion to card frauds every year, of which the vast majority is due to credit cards (71%). Debit card fraud losses claimed another 25% at \$2.7 billion, and prepaid cards 4%, or \$500 million.

Issuers Suffered \$10.9 Billion in Card Fraud Losses



The impact on fraud rates post EMV protocol implementation vary in different geographies. CNP fraud rose sharply in the wake of the shift of the liability and while increased use of 3-D secure technology helped curb this issue to an extent, fraudsters found different ways to operate.

THE RISE AND RISE OF CNP FRAUD

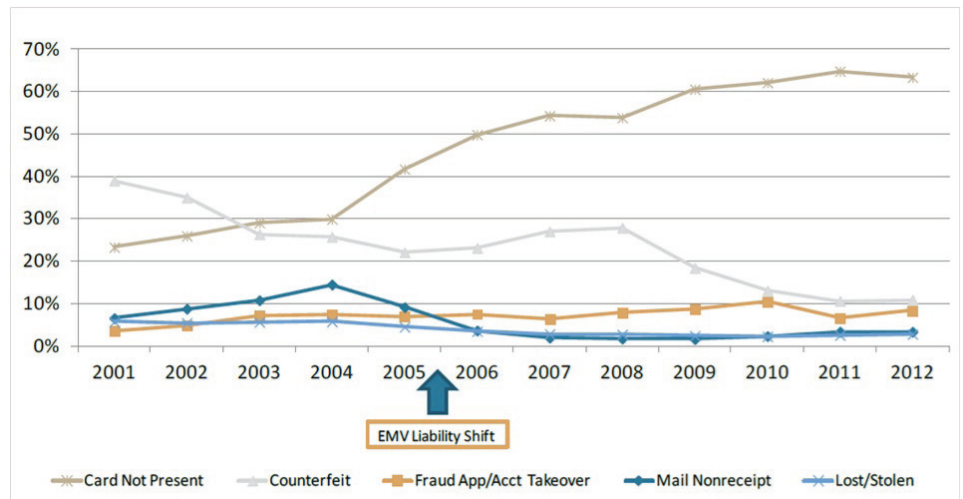
Card issuers are facing a tough time. U.S. credit card fraud is now a whopping 10 basis points, a 100% increase from just seven years ago. Rising card-not-present (CNP) fraud, stands at 45% of total U.S. card fraud currently. While reduced counterfeit fraud is good news for the issuers every other country that has adopted EMV has seen a precipitous increase in attacks on the CNP channels.

EMV's Impact on UK and Europe's Fraud Losses

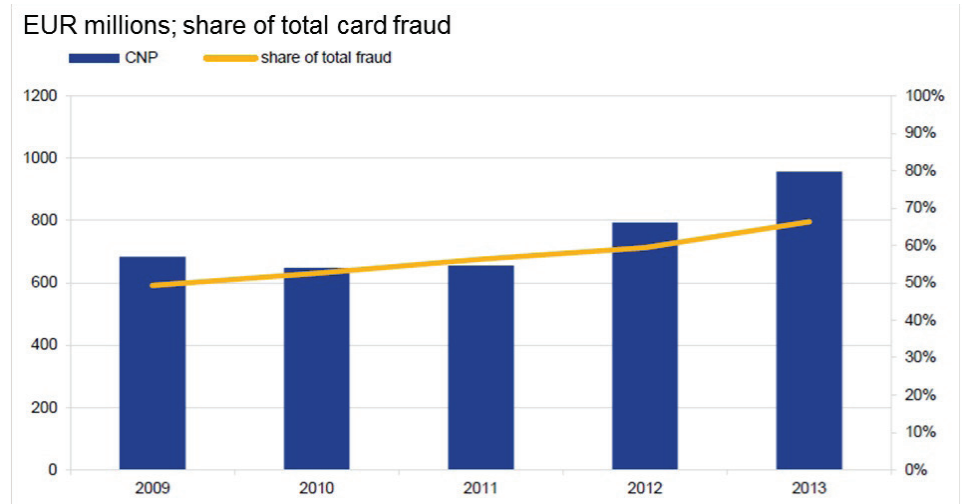
The UK and the rest of EU-27 were pioneers of EMV. The concept was being tested towards the end of 1998 in parts of Europe; however, the commencement of EMV system happened in the UK only in 2004. There was an immense growth in non-card based fraud while the card-based fraud reduced drastically. The EMV protocol, which tackles counterfeit fraud, and the PIN, which addresses lost/stolen fraud, had the desired effect and sharply curtailed counterfeit card fraud and lost/stolen fraud, both of which were at roughly the same level prior to the arrival of EMV.

For quite a while now criminals have found yet another avenue – ATMs. According to Financial Fraud Action UK, there were 7,525 incidents in the first four months of 2013, compared to 2,553 in a similar period the previous year. UK ATM fraud losses rose by 11% to GBP16.2 million in the first half of 2013, compared to GBP14.6 million in the first half of 2012.

Card Fraud in the UK, 2001-2012

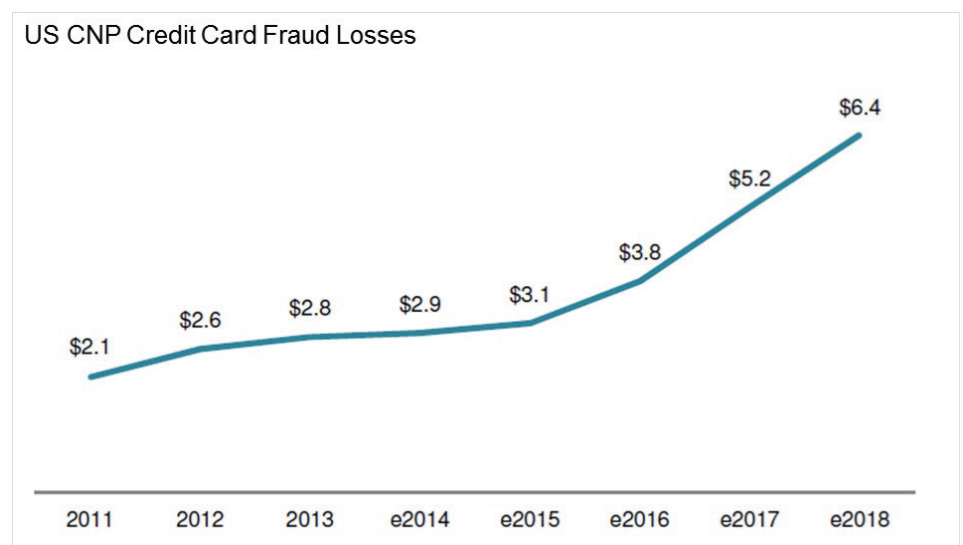


Europe saw through the implementation of EMV around the same time, but faced similar situations as UK. There was an immense growth in non-card-based fraud while card-based fraud reduced drastically.



EMV’s impact on USA’s fraud losses

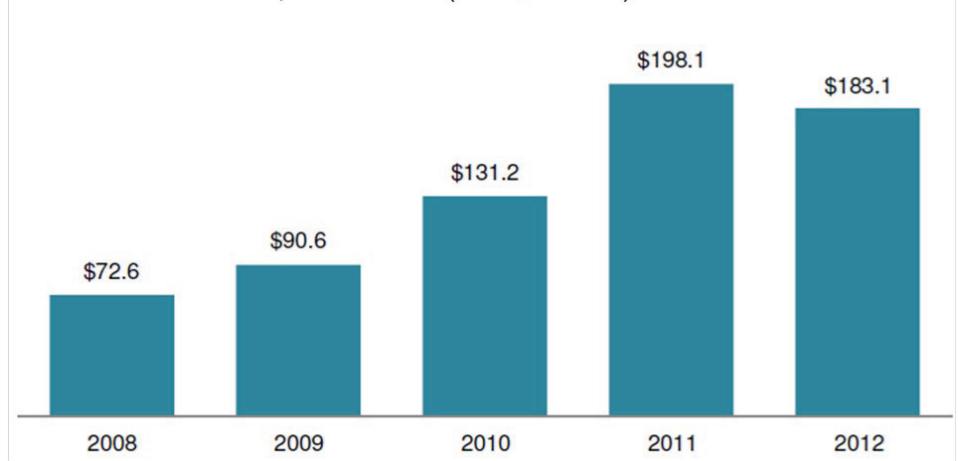
USA being a very fragmented market, the spike in CNP-based fraud will be quite large whose tremors could be felt across the world according to AITE reports. Cross-border counterfeit cards were a big chunk of the problem during migration as the country was still dependent on magnetic stripes. The growth rate in U.S. CNP credit card fraud was flat from 2012 to 2013, for the first time since the invention of online shopping. Even so, US CNP fraud losses will exceed US\$6 billion by 2018.



EMV’s Impact on Australia’s Fraud Losses

As the penetration of EMV-enabled cards and terminals progressed in Australia, banks began to see declining counterfeit losses on network-branded cards. However, like in the UK, Australia saw a sharp increase in CNP fraud losses as a result of both the growing popularity of digital commerce and a more fortified POS. CNP losses saw a slight decline in 2012 as merchants and issuers started deploying fraud analytics to detect CNP fraud and use tools such as 3-D Secure. The Australian government may issue a mandate of its own requiring 3-D Secure.

CNP Fraud in Australia, 2008 to 2012 (in AU\$ millions)



EMV IMPLEMENTATION: IMPACT AND INFERENCES

“Based on what we’ve seen in other regions that have migrated to EMV at in-store point-of-sale, fraud moves to other channels”

- Alisa Ellis,
VP - Global Products
& Solutions, Discover

EMV implementations across 80 countries have highlighted certain aspects that are more likely repercussions.

- **EMV implementation will shift the fraud landscape towards application fraud, account takeovers, counterfeiting cards and CNP environments.**
- **Friction between retailers, payment card networks and issuing institutions will rise in the form of more lawsuits.**
- **Most data breaches will continue to occur at small enterprises and go unnoticed, despite the media’s unrelenting attention on major retailers.**
- **False positives will keep driving away customers, giving banks the impetus they need to invest in fraud detection solutions and strategies to improve card authorization practices.**
- **Regulatory institutions such as the FFIEC, CFPB, and FTC will play a bigger role in fraud mitigation and cyber security.**
- **Pending legislation will determine liability for data breaches among retailers, payment card networks and issuing institutions.**

The most likely solution to the issue is to understand that a point solution will not hold good for thwarting CNP fraud or any other kind of fraud arising after implementation of EMV. Financial Institutions, merchants and issuers have to work together to keep customer data safe and upgrade their defenses.

The arrival of EMV will certainly help curb some types of fraud including counterfeit fraud, but the experience of other countries shows that the arrival of EMV will do nothing to stop database breaches, and CNP fraud will rise precipitously unless preventive measures such as tokenization, behavioral analytics, 3-D Secure and real-time cross-channel fraud management systems are implemented.

Though liabilities will shift, it must be kept in mind that trust is paramount for banks, merchants and issuers. If they have to continue to protect financial security and maintain credibility, they need to create an environment of trust and safekeeping by implementing proactive, intuitive and intelligent fraud prevention strategies.

This report contains information on EMV and its effective implementation. The information provided is not advice, and should not be treated as such. All trademarks acknowledged to their respective owners. CustomerXPs and Clari5 logos are registered trademarks of CustomerXPs Software.

References

- Aite Report 2014 – Lessons Learned and the US Outlook
- Aite Report 2014 prepared for RSA - Card-Not-Present Fraud in a Post-EMV Environment: Combating the Fraud Spike
- Mercator Advisory Group Report 2014 – EMV Adoption & Its Impact On Fraud Management Worldwide
- Congressional Research Service May 2016 - The EMV Chip Card Transition: Background, Status, and Issues for Congress by Patricia Moloney Figliola (Specialist in Internet and Telecommunications Policy)
- State of Card Fraud 2016 powered by Ripplshot

About the author





KARUNAKAR MOHAPATRA


Karunakar is a Research Analyst at CustomerXPs. He monitors developments in the BFSI technology domain and publishes significant trends that impact the sector. You can find Karunakar on [LinkedIn](#).


About CustomerXPs

CustomerXPs is an enterprise software product company offering Enterprise Financial Crime Management (EFCM), Anti-money Laundering (AML) and Customer Experience Management (CEM) products for Tier-1 global banks. CustomerXPs is revolutionizing Fraud Management and Customer Experience Management in Fortune 500 banks by harnessing the power of extreme real-time, cross-channel intelligence. Voted 'Best Fraud Detection Product 2016' by OpRisk / Risk.net, CustomerXPs' flagship product Clari5's differentiated approach deploys a well-synchronized, context-aware 'central nervous system' in banks with the ability to stop fraudulent transactions with real-time, actionable insights.

 clari5@customerxps.com

 [/company/customerxps](https://www.linkedin.com/company/customerxps)

 [/customerxps](https://twitter.com/customerxps)

 customerxps.com

