EMV Adoption in the U.S.

What you need to know about the outcome of EMV adoption in other countries and the implications for adoption in the U.S.

Powered By
rippleshot

Table of Contents

Introduction

Four decades ago, payment card magnetic stripe technology revolutionized the way we make purchases, accelerating the proliferation of the global credit card industry. Now, EMV-enabled cards, named after its original developers: Europay, MasterCard, and Visa, are quickly becoming **the new global standard** for authorizing payment card transactions. EMV cards feature an embedded microprocessor chip rather than a magnetic stripe that stores encrypted cardholder data.

While most developed countries have adopted the EMV standard over the past decade, the U.S. is the last developed country that has continued to rely on magnetic stripe cards. However, the opportunity to improve security for cardholders and EMV adoption in other countries is prompting the U.S. to accelerate adoption of EMV technology.

Our whitepaper will explore **the benefits and challenges of adopting EMV standards**. We will also look at the **expected impact on fraud losses** of the quickly approaching EMV rollout in the U.S.

What is EMV?

EMV utilizes a small data processing chip embedded in either plastic or a mobile device to transmit encrypted cardholder information, including cardholder’s name, card number, and expiration date. In an EMV transaction, the cardholder touches the plated contact point of the card to an EMV reader or waves the card/mobile device within 4 centimeters of an EMV reader. The EMV reader powers the embedded chip, allowing it to communicate encrypted cardholder information, and generating a code to send to the processing host for verification.

The host processor decodes the encryption, verifies the EMV chip and returns an authorization code to allow the transaction, providing **dynamic authentication**. The EMV chip and the card/mobile device holder’s PIN (chip-and-pin), or signature (chip-and-signature) must be verified in order for the transaction to be valid, creating a 2-factor authentication.

What is EMV?

An EMV-enabled card is more secure than a magnetic stripe card as it allows for dynamic authentication, whereas data on a traditional magnetic stripe card is static.

Static data from magnetic stripe cards can be easily copied (skimmed) with a simple card reading device and used to make counterfeit cards. EMV-enabled cards create one-time authorization codes for each transaction, making counterfeit fraud much harder.

Chip-and-pin cards create a second level of security through the requirement of a customer to enter a PIN for each transaction, which is more effective in preventing fraud than signature verification used with magnetic stripe cards.

Benefits of EMV-Compliant Cards

More secure card-present (CP) transactions:
EMV has been proven to reduce card-present fraud in which customer account information is copied from a card's magnetic strip and then transferred to a counterfeit card for fraudulent purchases, protecting consumers from fraud and identity theft, saving issuers from fraud losses, and saving merchants from lost business. Further, it will prevent the U.S. from becoming a target for "cross-border" counterfeiting in which fraudsters use the cards in a non-EMV compliant country.

Greater interoperability between countries:
EMV is the standard in most developed countries outside the U.S. Thus, American travelers would be able to use their cards when traveling internationally, and foreign travelers would also be able to use their cards when traveling in the U.S. This is lucrative for both issuers and merchants as it will encourage additional card spending.

New revenue sources:
Card brands could derive new revenue sources via marketing offers and loyalty programs that can be transmitted directly from the merchant to the card / mobile device through the EMV chip.

Accelerating mobile payment solutions:
EMV and Near Field Communications (NFC)-enabled mobile payment technologies require a similar back-end infrastructure. Thus, EMV point-of-sale (POS) terminals will also be able to accept NFC transactions from mobile devices, allowing merchants to have one POS terminal for multiple types of payment, and providing more convenience and speedier checkout to consumers.

Downside of EMV-Compliant Cards

Rise in other types of fraud:

EMV adoption has been proven to reduce card-present fraud, however, other types of fraud will rise in its place. Overall fraud losses will not be reduced as card-not-present fraud (CNP) and fraud targeting banks is expected to rise.

High cost of EMV compliance:

Purchasing or upgrading existing POS terminals and systems will be expensive. Javelin Strategy & Research estimates the cost of replacing POS terminals will be $6.75B, cost of replacing cards will be $1.4B, and cost of replacing ATMs will be $500M; The total price tag of EMV migration totals to $8.7M, compared with estimated savings to issuers of $700M in card fraud losses annually. Smaller merchants who might go 5-10 years between replacing terminals, and experience relatively low levels of fraud may view EMV terminals as a costly and unnecessary expense.

Replacing POS Terminals: **$6.75 billion**

Replacing Cards: **$1.4 billion**

Replacing ATMs: **$500 million**

[7]

U.S. Adoption Timeline

October 2015: Deadline for Merchants
October 2017: Deadline for Gasoline Retailers

EMV adoption in the U.S. has been slower than in other countries as the U.S. payment system infrastructure is substantially more complex and diverse, and the U.S. already has an online authorization process. However, all major card brands (Visa, MasterCard, American Express, and Discover) have announced roadmaps to transition to the new EMV standard in the U.S., and have set October 2015 as the deadline for merchants, and October 2017 as the deadline for gasoline retailers.

The card brands' deadline serves as an incentive rather than a mandate to switch to EMV; **after the deadline, the liability for card fraud will switch from card issuers to whichever party (either issuer or merchant) is using non-EMV compliant devices**. If both the issuer and the merchant are EMV compliant, the issuer will still bear liability for the fraud. Thus, the card brand deadline is intended to incentivize issuers to update their cards and merchants to update their POS terminals for EMV compliance, as liability will be shifted to the party that continues to use the old system.

U.S. Adoption Timeline

Due to the cost and complexity of PIN-based authentication, U.S. implementation will not be a true chip-and-PIN solution yet.

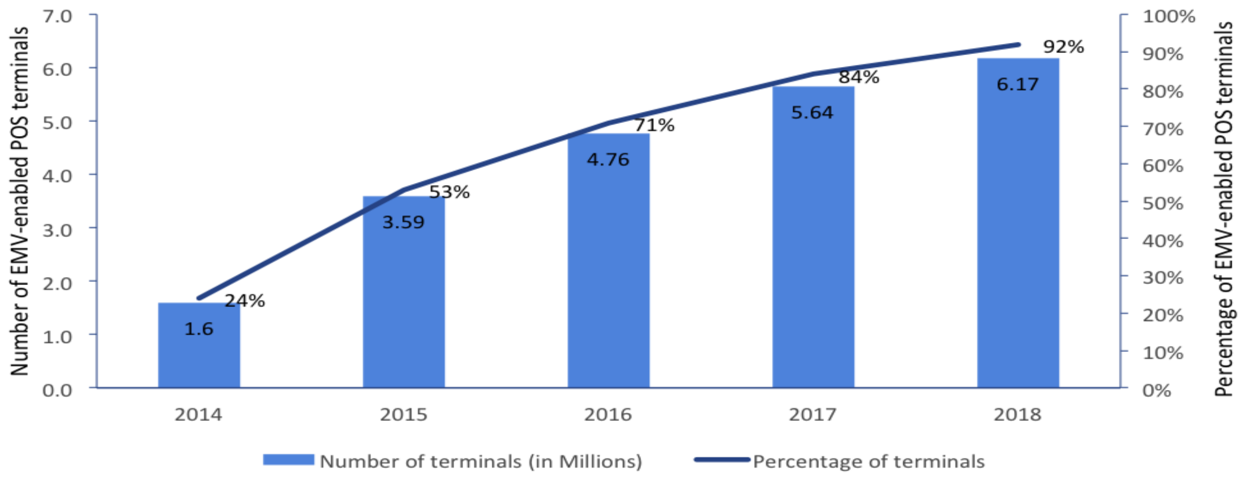
At launch, card brands' roadmaps do not require POS terminals to accept a PIN from the cardholder, but rather will be set up to accept a signature to verify the card details (chip-and-signature).

Use of a meaningless signature that merchants don't really verify, rather than a PIN, disables the second layer of security the chip-and-pin system is intended to create.

The cost and complexity of upgrading and replacing POS terminals also means that it will likely take 2-5 years before there is critical mass of merchants which are EMV-compliant.

Forecast for percentage and total number of EMV-enabled terminals in U.S.

Source: Javelin Strategy & Research, 2014



[9]

Impact on Global Fraud Trends

To understand the potential implications of EMV adoption in the U.S., it's helpful to examine the impact of EMV adoption in other countries.

United Kingdom:

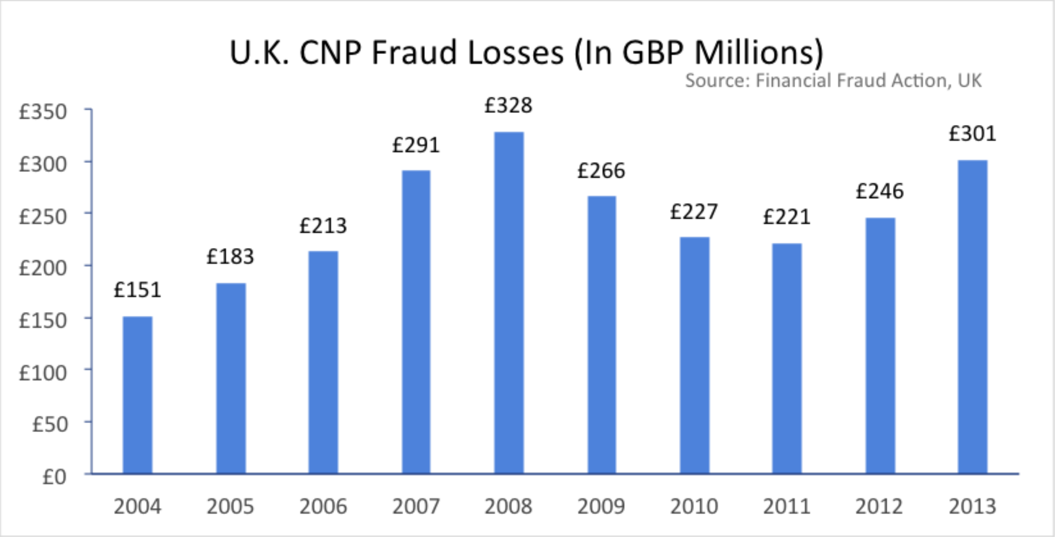
The EMV standard was first implemented a decade ago in the U.K. as card fraud was considerably higher than in the U.S., primarily because of a time lag between transaction and authorization due to an offline authorization process driven by a costly telecommunications structure. The liability shift in the U.K occurred in January 2005.

The adoption of EMV in the U.K. has been successful at reducing card-present (CP) fraud in which a physical card is presented for a transaction. Counterfeit and lost/stolen fraud losses fell 56% from £97M to £43M and 34% from £89M to £59M, respectively from 2005 to 2013. Much of the remaining fraud is "cross-border" counterfeiting, which is expected to decline as more countries adopt the EMV standard.

However, after adoption there has been an even greater increase in card-not-present (CNP) fraud which cannot take advantage of the EMV chip. **CNP fraud losses increased 79%** from £183M in 2005 to a peak of £328M in 2008. In response, issuers and merchants developed and implemented 3D Secure technology and more sophisticated fraud analytics, managing to deflate fraud losses to £221M in 2011. However as fraudsters have started to target softer targets such as call centers and the volume of e-commerce transactions continue to rise, **fraud losses have begun to rise again, reaching £301M in 2013.**

[10]

Impact on Global Fraud Trends

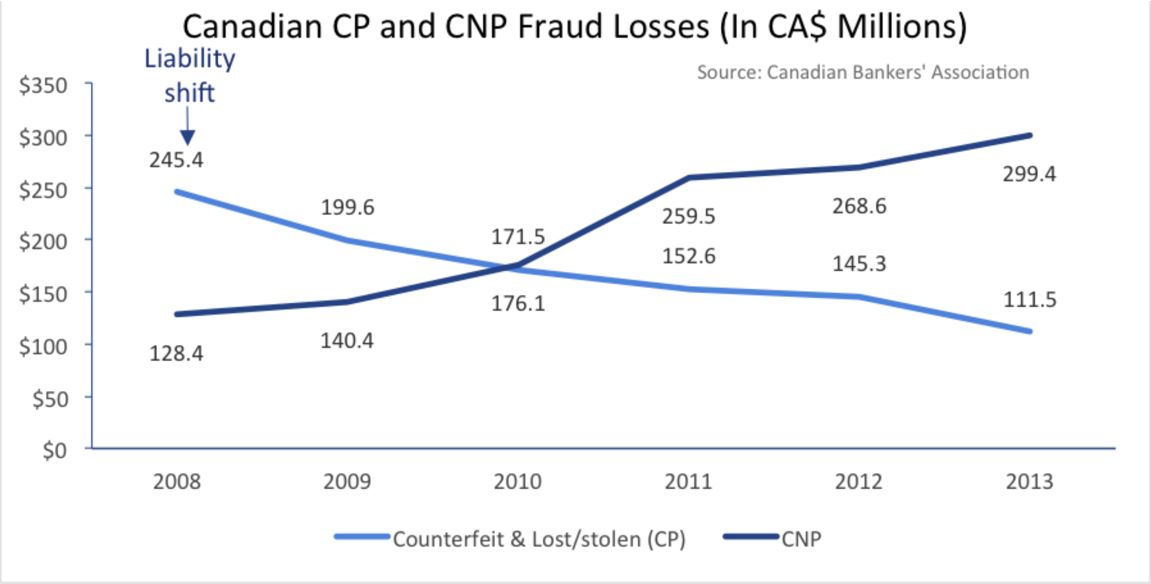


In addition to the rise of CNP fraud, EMV adoption also led to a dramatic rise in fraudulent new accounts and account takeovers in the U.K.

Losses from card ID theft rose 51% from £31M in 2005 to £47M in 2008.

As fraudsters were no longer able to steal card data easily at POS, their next best option was to get the cards directly from the bank by stealing an identity and applying for a new account or taking over an existing account and getting cards mailed to them. Due to similar responses from issuers in more sophisticated fraud analytics, fraud losses declined to £23M in 2011. However, as with CNP, fraud losses have begun to rise again, reaching £32M in 2012.

Impact on Global Fraud Trends



Canadian CP and CNP Fraud Losses (In CA$ Millions)

Source: Canadian Bankers' Association

Canada:

The adoption of EMV in Canada in 2008 resulted in a similar shift from CP fraud to CNP fraud.

CP fraud losses fell 54% from $245M in 2008 to $112M in 2013, while **CNP fraud more than doubled (133%) from $128M in 2008 to $299M in 2013.**

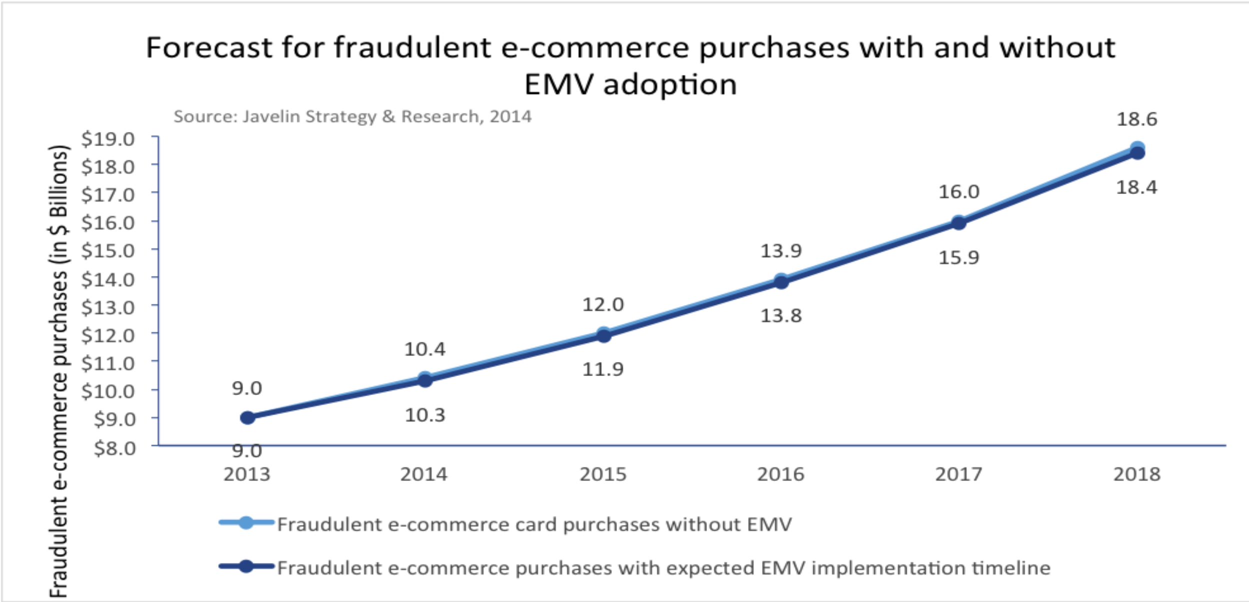
Implications for U.S.

As a result of the adoption in the U.S., CP fraud loss is expected to decline as it has in other countries. However, the decline will less be dramatic than the U.K. as the U.S. already has an online real-time authentication process in place, and as the U.S. is expected to implement less secure chip-and-signature cards rather than more secure chip-and-pin cards.

The U.S. should also expect to see a spike in CNP fraud losses and fraudulent new account or account takeovers similar to other countries as fraud shifts from CP to CNP channels.

Further, online spending in the U.S. is expected to rise from $262B in 2013 to $440B by 2017, at a compounded annual growth rate of 13.8%. The increase in e-commerce transaction volume combined with the EMV rollout is expected to dramatically increase CNP fraud.

CNP fraud is expected to be nearly 4 times greater than POS fraud in 2018 largely driven by the increased e-commerce transactions.



Forecast for fraudulent e-commerce purchases with and without EMV adoption

Source: Javelin Strategy & Research, 2014

[13]

Conclusion

Migrating to EMV has become necessary for the U.S. as the rest of the world is quickly adopting this standard. The U.S. payments industry stands to reap the benefits of reduced risk of becoming a global fraud target, increased revenues from travelers and new revenue streams, accelerated acceptance of mobile payments, and improved customer satisfaction through EMV adoption.

However, the aftermath of EMV adoption in other countries and U.S. fraud trends indicate adoption of EMV in the U.S. will do little to reduce the impact of data breaches and overall fraud losses.

Fraud is simply expected to shift from CP to online and other CNP channels that cannot take advantage of the EMV chip, or other areas of vulnerability in the payment industry.

Conclusion

This fraud will be compounded as online transactions continue to grow. Hence, it will be essential for issuers and merchants to anticipate and take measures to protect against vulnerabilities in other products or channels that fraudsters could take advantage of.

- **Additional security layer for CNP transactions:** Use of additional authentication at the time of a purchase through a password can help to verify the cardholder identity.
- **Tokenization:** Use of tokenization encrypts data once it enters the merchant and issuer system to help protect cardholder data when a data breach occurs.
- **Sophisticated fraud analysis tools:** Use of fraud analytics can help to detect patterns indicative of attacks that are imminent or underway, and identify cards at high risk for fraud. Even with preventative measures such as a second security layer and tokenization, data breaches and CNP fraud will be inevitable. Sophisticated fraud analytic tools can help mitigate losses when breaches occur.

As with any type of fraud prevention, no single point solution will suffice. Merchants and issuers will have to take a layered approach to protect against fraud losses.

Rippleshot detects data breaches faster, allowing card issuers, processors and merchants to proactively monitor suspicious activities and implement smarter fraud risk management strategies when breaches do occur. Rippleshot knows that what you can't see can hurt you, which is why we sweat the small stuff - the ripples before the tsunami, the tiny anomalies that signal a looming data breach - and let you know earlier, so you can play a pivotal role in reducing fraud loss, improving cardholder security and reducing the severity of breaches.