EXECUTIVE INSIGHT

August 2015

12 Clock Tower Place, Suite 150 | Maynard, MA 01754
www.mercatoradvisorygroup.com | phone: 1(781) 419-1700 e-mail: info@mercatoradvisorygroup.com

ARE THE U.S. CHIP RULES ENOUGH?

A longer term view of security and the payments landscape is needed.

Abstract: The United States is finally modernizing its card payment systems and confronting fraud with rules regarding use of the global EMV chip card standard starting on October 1, 2015. Unfortunately, there's a lot more to be done before we can say the U.S. payment system is up to speed with the rest of the world on chip card security. And given the focus on "chip" by itself, it will be a long time before overall fraud losses are reduced and consumer fears about data compromise addressed. Decisions and investments made today should take a longer term view of security and the payments landscape.

Arthur D. Kranzley
Director Emeritus

Art has over 40 years of financial services experience, including as executive advisor in advanced and emerging payment technologies, assisting companies in the areas of authentication, security, electronic commerce, mobile commerce, smart card, and credit/debit payments.

What is happening now?

On October 1, 2015, payment network versions of a chip card liability shift become effective for participants in many of the major credit and debit networks in the United States, including MasterCard, Visa, American Express, and Discover. However, there is no mandate for chip cards or terminals, no established timetable or rollout schedule, and no sunset date for magnetic stripe acceptance at point-of-sale (POS), ATM, or automated fuel dispenser devices. Moreover, there is no consideration for other types of fraud that could increase as the result of fraud migrating to other vulnerable areas. These areas include lost, stolen, and card non-receipt fraud, overseas fraud, and fraud moving to card-not-present channels including online shopping.

The payment network liability shift rules are not a call or mandate for chip as was the case in other parts of the world, including Europe and Canada. In Europe, the European Payments Council published the Single Euro Payments Area Cards Framework (SCF) in 2009 establishing principles and rules to ensure a homogeneous experience for both cardholders and merchants at the point of sale and ATMs. As part of this framework, EMV chip and PIN became the standard for card payments. Likewise, in Canada, the Interac Association, responsible for the national debit network, established sunset dates when magnetic stripe debit cards would not be accepted at automated banking machines after 2012 and at the POS after 2015, effectively requiring all cards to be chip-and-PIN enabled.

In the U.S., the EMV chip liability shift rules are intended to encourage issuers to provide cardholders with EMV chip cards and to motivate merchants to install and enable EMV point-of-sale devices. Today, issuers are financially responsible for all transactions initiated with a card present at a POS device, including counterfeit cards. With the liability shift rule, if a card has been issued with a chip and a fraudulent copy of that card's magnetic stripe is used at a merchant without chip POS support, the merchant is liable for that transaction. However, not all networks have a corresponding rule for chip-and-PIN based transactions, so the liability shift will not always apply to lost or stolen or card non-receipt fraud. Also, details have not been made clear to the industry for those networks that will apply a liability shift to lost or stolen cards for chip-and-PIN transactions.

What else should be done?

Credit and debit card fraud is the top security concern among U.S. consumers today, topping worries about identity theft and national security. Nearly 60% of American consumers would be less likely to continue using a bank or merchant following a security breach.[i]

Continued dependence on magnetic stripe card technology developed in the early 1970s is part of the reason counterfeit fraud is so high in the United States. Counterfeit fraud now amounts to 37% of all U.S. credit card fraud and continues to escalate.[ii] In contrast, in the United Kingdom counterfeit fraud dropped 63% and lost/stolen

fraud dropped 48% between 2004 and 2014 once chip-and-PIN came into use.[iii] Similarly, while deploying chip-and-PIN, Canada saw a drop of 68% in domestic counterfeit fraud and a drop of 44% in lost/stolen fraud (2008 to 2014).[iv]

In May 2015, EMVCo announced a healthy growth rate of 43% in EMV chip cards issued during 2014, bringing the total number of chip cards to 3.4 billion worldwide, with 32% of all card-present transactions globally being chip. At the end of 2014, the percentage of card-present transactions in Europe that were EMV chip was 96.6%; in Canada, Latin America, and the Caribbean, it was 85.41%; in Africa and the Middle East, it was 80.0%; and in Asia Pacific, it was 27.01%. In the United States, EMV chip transactions were an insignificant 0.12% during the same period.[v]

The world is moving to EMV chip and PIN, and the U.S. needs to harmonize its card payment systems quickly or the U.S. will bear the majority of global fraud. Rollout of chip-and-signature in the U.S. over the next 5+ years will do little to address overall card fraud, based on global market experiences. Any EMV program must be coupled with a comprehensive multichannel and multilevel fraud management plan including strong cardholder authentication at the point of sale (e.g., chip and PIN), secure cardholder authentication online, encryption, tokenization, and remote transaction security. For example, it has been noted that EMV is indirectly driving some major merchants to review and upgrade their entire point-of-sale and transaction processing systems to incorporate end-to-end encryption, tokenization, and other technology enhancements.

Historically, markets with successful EMV chip programs reduced counterfeit and lost/stolen fraud but suffered significant increases in cross-border card fraud and remote or card-not-present (CNP) fraud, including online fraud. In the U.K., CNP fraud skyrocketed by 186% between 2004 and 2014, as did fraud abroad with an increase of 162%.[vi] In Canada, between 2008 and 2014, CNP fraud grew by 180% and cross-border counterfeit grew by 118%.[vii] In real dollars, these increases were approximately double the savings in counterfeit and lost/stolen fraud in the same period (182% in U.K. and 206% in Canada).

What are retailers considering?

Recent account data compromises at major retailers (Target, Home Depot, and others) exposed over 100 million credit card accounts in 2014. To payment networks, banks, and retailers, this was a catalyst to begin implementing the global EMV chip card technology in the United States. However, the traditional terminal upgrade cycle is 5 to 7 years and many POS systems will not be chip-enabled until 2020 or later. This is particularly true for midsized and smaller merchants (Levels 2, 3, 4). Fortunately, Level 1 merchants are promising to replace systems earlier, but it remains to be seen how many will be able to meet all of the requirements in the next several years, particularly since some are reengineering their entire systems to incorporate other security and marketing functions as discussed earlier.

The National Retail Federation (NRF) has publicly supported EMV chip in the U.S. but believes that banks and payment systems should be more in line with global standards. NRF has taken a strong position on the need for implementation of both chip and PIN as the U.S. standard. According to the NRF, upgrading the POS infrastructure to support chip cards will require significant investment by merchants, costing $20–30 billion. This cost may increase as other enhancements needed for the future are implemented concurrently with EMV support.

In addition to replacing or updating terminal hardware for 14 million POS devices at U.S. merchants, chip support will require software upgrades, functional testing, security evaluation, and certification to support each payment brand. This is further complicated by challenges in how the industry will incorporate online debit support with chip and PIN at the POS in adherence with the debit routing regulatory requirement of the Durbin Amendment. The expense of upgrading to chip terminals also comes at a time when merchants are rolling out alternative payment and shopping technologies such as mobile payments, Near Field Communication (NFC), beacons, and location-based marketing systems, enhanced loyalty and reward programs, and proprietary and merchant-based payment systems. Merchants must ensure that any investments made now in terminals and systems are flexible enough to incorporate future add-ons.

What should issuers be concerned about?

Issuing cards with chip, developing the systems support for authorization of chip transactions, and educating cardholders are certainly some of the major tasks that issuers need to complete as part of their chip migration plans. As with any new payment product or system, consumers are likely to be confused about chip cards in terms of what they protect and how they work. Setting proper expectations and educating cardholders about use of chip cards in the U.S. and abroad will be a challenge. It may be tempting to represent the new chip card as a solution to account data compromise and a way to protect private information, even though this should not be promised as long as magnetic stripe transactions will outnumber chip transactions for several years to come.

More important will be the establishment of a strategic framework and implementation plan to address overall card fraud that will maximize results from investments in chip and corresponding system upgrades. Chip cards address only counterfeit fraud; they do so by using a dynamic cryptogram to authenticate the card. Issuing chip cards should be just part of a broader payments security framework addressing cardholder authentication not only at the POS and but also via remote payment channels including telephone order/mail order, online, and mobile.

At the POS, unauthorized use of lost, stolen, and non-received cards will grow without the use of PIN. In addition, the absence of a PIN will cause acceptance problems in chip-and-PIN markets, particularly at unattended terminals, self-service checkout devices, and merchants locations where staff may not understand how or be willing to accept chip-and-signature cards.

In card-not-present channels, there are multiple authentication solutions for issuers that should be integrated with chip rollout plans. These include risk-based authentication using fraud analytic tools, dual-channel one time passwords (OTPs) through SMS and email messages, OTPs via secure fob devices, Chip Authentication Program (CAP) readers and mobile devices, challenge-response solutions, virtual accounts, wallets, and tokens to name a few. Industry efforts on developing and expanding standardized protocols will reduce CNP fraud by enabling issuers to deploy their own strong cardholder authentication programs on merchant Internet and mobile shopping sites.

Conclusion

It's great news that the U.S. card payments industry is moving toward EMV chip to address counterfeit fraud at the POS. This is somewhat consistent with earlier and ongoing implementations of chip around the rest of the world and is a positive step in harmonizing card security in the U.S. with global standards. However, as experience abroad has shown, a more comprehensive security framework addressing all payment channels as well as cardholder authentication needs to be established and implemented on a national scale by the payment brands, processors, issuers, and merchants. Investments in securing and modernizing the payments infrastructure with chip support are steep and should be leveraged to address future requirements when looking a decade ahead. As an industry, we must live with choices made today for a long time.

Endnotes

[i] 2014 Unisys Security Index.

[ii] http://www.mastercard.com/us/company/en/docs/Modeling_white_paper.pdf

[iii] UK Cards Association.

[iv] Interac Association.

[v] EMVCo, LLC. EMVCo is the global technical organization owned by MasterCard, Visa, JCB, American Express, Discover, and UnionPay established to manage the EMV specification and to promote the interoperability of chip cards and terminals worldwide.

[vi] Financial Fraud Action UK Plastic Fraud Figures

[vii] Canadian Bankers Association

For more information about this report, please contact:

Arthur D. Kranzley, Director Emeritus
akranzley@mercatoradvisorygroup.com

Mercator Advisory Group is the leading independent research and advisory services firm exclusively focused on the payments and banking industries. We deliver a unique blend of services designed to help clients uncover the most lucrative opportunities to maximize revenue growth and contain costs.

Advisory Services. Unparalleled independent and objective analysis in research documents and advice provided by our Banking Channels, Credit, Commercial and Enterprise Payments, Debit, Emerging Technologies, Global Payments, and Prepaid practices.

CustomerMonitor Survey Series. Eight annual Insight reports based on primary data from Mercator Advisory Group's bi-annual surveys of 3,000 U.S. adult consumers to determine their behavior, use, preferences, and adoption of current and emerging payment methods and banking channels to help our clients identify and evaluate business opportunities and make critical business decisions.

Consulting Services. Services enabling clients to gain actionable insights, implement more effective strategies, and accelerate go-to-market plans. Offerings include tailored project-based expertise, customized primary research, go-to-market collateral, market sizing, competitive intelligence, and payments industry training.

PaymentsJournal.com. The industry's only free online payments and banking news information portal delivering focused content, expert insights, and timely news.

For additional copies of this report or any questions, contact Mercator Advisory Group at 781-419-1700.