BERKERYNOYES
INVESTMENT BANKERS

Payments 2014:

How EMV Migration is Poised to Change the U.S. Market Landscape

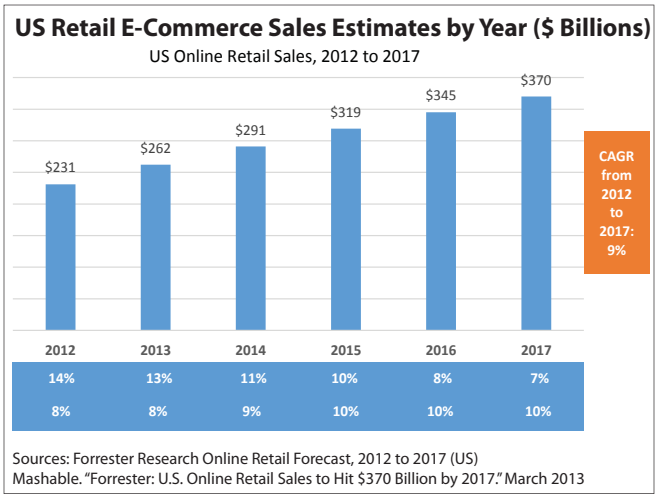
White Paper

John Guzzo, Managing Director
Peter Ognibene, Managing Director

Introduction

Over the past year, credit card and customer information breaches in major U.S. retailers Target and Neiman Marcus, as well as the restaurant chain P.F. Chang's, have made national headlines. The effects of these breaches, which include the potential exposure of one-third of Americans' credit card or personal information,[1] propelled the issue of credit card security into the national consciousness.

In line with this heightened focus on credit card security, the U.S. will shift over to new Europay, Mastercard, and Visa (EMV) standards. This is set to take effect in October 2015, making the U.S. the last major industrialized nation to completely adopt the standards.



Sources: Forrester Research Online Retail Forecast, 2012 to 2017 (US)
Mashable. "Forrester: U.S. Online Retail Sales to Hit $370 Billion by 2017." March 2013

EMV Background

These new standards, which require payment systems with chip and pin technology, aim to mitigate fraudulent transactions. This technology uses a highly-secure, microprocessor-embedded chip which is extremely more difficult to clone than the decades-old magnetic strip. Additionally, the standards require customers to enter a pin during the transaction process – a feature more secure than a signature. In order to complete the transition to full EMV standards, credit and debit card providers need to issue the new cards, while merchants have to upgrade to EMV-compatible systems.[2]

With regard to liability issues, the new EMV standards will transfer liability for fraudulent purchases from credit card acquirers and processors to merchants if merchants do not switch to EMV-compatible systems. For some smaller companies, the switch may be as simple as attaching a keypad to existing POS terminals. However, for larger merchants, the process could involve an extensive overhaul of existing payment infrastructure.[2]

Moderate estimates anticipate that this transition will take about three to five years to complete. By the 2015 deadline, approximately 25% of chip-enabled credit and debit cards will be in issuance.[3] Full issuance is not expected to be realized until 2018. In terms of merchant readiness, approximately half of all locations are projected to be EMV-ready by the October 2015 liability shift date.

This infrastructure includes EMV-capable terminals, as well as updated software capable of processing the higher volumes of data. The adoption of such infrastructure also requires numerous levels of hardware and software compliance testing to ensure a smooth transition.[4]

One of the most notable examples of merchant preparation involves the tech giant Apple Inc.'s deal with the payment processor VeriFone Systems, Inc. to outfit Apple's mPOS terminal with EMV-compatible technology. Apple could serve as a catalyst by prompting other merchants to adapt EMV infrastructure in advance of the October 2015 deadline.[3] In doing so, it may in turn encourage banks to accelerate issuance of chip and pin-ready cards to maintain their "leading-edge" profiles and gain a competitive edge. With regard to systems providers such as VeriFone, these companies stand to reap substantial profits from a widespread demand for new infrastructure.

As systems providers attempt to offer EMV-capable technology to merchants, they must compete over an estimated $2.6 billion market during the next five years.[3] This estimate does not include the numerous software demands of EMV migration, which range from the aforementioned compliance testing to consumer coaching systems.

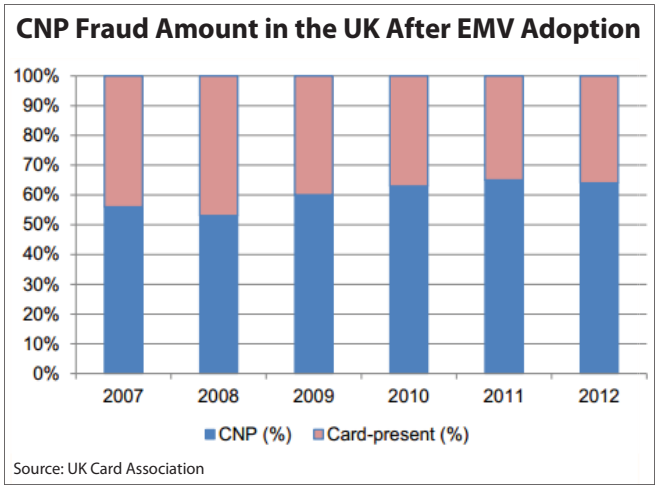
To gain a competitive edge, processing companies could benefit from acquiring and consolidating the best and most cost effective technology, which may lead to an increase in M&A activity. The payments M&A market has been robust over the past few years, as transaction volume and multiples continue to rise.

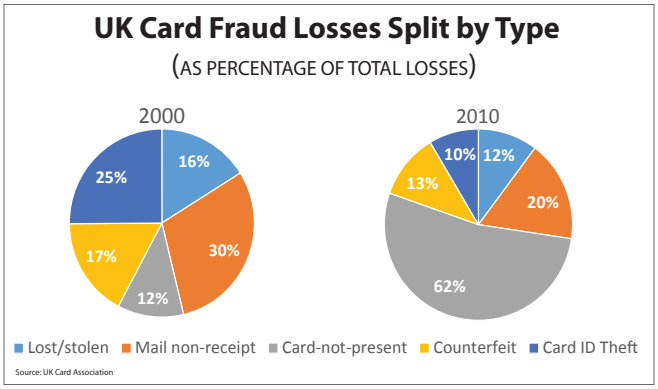
Fraud Migration to Card-Not-Present (CNP)

In addition to the obvious hardware upgrades, EMV migration can significantly impact other business segments. Full usage and acceptance of EMV-enabled systems will make in-person payments fraud more difficult and unprofitable. Therefore, fraudsters will typically migrate to the path of least resistance, resulting in an increase in online payments fraud, also known as card-not-present or CNP. This trend has occurred in other countries that have already migrated to EMV standards.

For example, CNP fraud tripled in the U.K. during EMV deployment period from 2000-2010, with an annual increase from £72.9M to £226.9M.[5] Likewise, Australia and France have witnessed significant increases in CNP fraud during their migration to EMV standards.[6] As EMV standards approach full usage and acceptance during the next three to five years, CNP fraud in the U.S. will likely rise.

In terms of liability for CNP fraud, merchants are required to cover fraudulent transactions.[7] This is problematic because online fraud costs much more than a direct loss of goods and services. Merchants must shoulder overhead and replacement costs for their items, in addition to charge-back fees from credit card providers. There is also a general consensus that eCommerce will continue to grow at a healthy rate, which will further expose merchants to CNP fraud.[5] To make matters worse, LexisNexis discovered that one in three consumers who were victims of fraud avoid certain merchants; one in four consumers report that they spend less money; and almost one in three report switching payment methods. Thus, card providers and especially merchants have aligned interests in reducing fraud.[8] The proliferation of eCommerce and the imminent shift to EMV pose obvious concerns for merchants and card providers, who would be wise to examine their risk management procedures before the full onset of fraud increases.





Although credit card companies and merchants have measures in place to reduce fraud related risk, they are attempting to refrain from overly complicating the consumer transaction experience in order to prevent the frustration that leads to lower sales volume. Briefly consider Amazon's One-Click checkout, as opposed to a system that redirects consumers to third-party security sites and requires them to pre-confirm their purchase via email or text. In this scenario, it is obvious that merchants benefit from maintaining a streamlined checkout experience for their customers. With this challenge in mind, there is great opportunity for companies who provide discreet and effective fraud-detection technology. For card providers and merchants, the possession of secure and streamlined technology should provide a competitive edge.

Mobile

In addition to increased CNP fraud, EMV migration is expected to usher in a significant but less apparent impact regarding the mobile payments industry. In the past, the lack of a critical mass of contactless terminals impeded the expansion of mobile payments usage. During EMV migration, many EMV-capable systems will arrive equipped with contactless payment technology.[5] Therefore, the overhaul of payment terminals will provide the technological ecosystem for the mobile payments industry to flourish. For merchants, the benefits of mobile payments are numerous.

They offer quicker and more secure transactions with reduced fees in some cases. Furthermore, they provide merchants with real-time inventory and customer behavior while enhancing the shopping experience with additional features such as sales offers, rewards programs, and coupons.[9]

Another complimentary development in mobile payments landscape, the acceptance of host card emulation (HCE) by MasterCard and Visa, will further facilitate the expansion of mobile payments. HCE allows credit card information to be stored in the cloud instead of the secure chips embedded in phones. This could undermine the control that service providers like Verizon and AT&T have been using to block services such as Google Wallet in order to promote their own mobile payments solution, Isis.[10] Thus, the acceptance of HCE by MasterCard and Visa will promote a level playing field for emerging mobile payments companies.

Currently, there is no dominant player in the mobile payments industry, but giants like Google and PayPal are vying for control. It is also important to note that mobile payments alone may not provide a value-added service for consumers. However, companies that can integrate a full range of products with their mobile payments platform provide a compelling reason for both consumers and merchants to adopt the technology.

The Potential Impact on M&A

From a mergers and acquisitions (M&A) perspective, the payments market should expect to see many strategic acquisitions throughout the deployment of EMV-technology. As mentioned earlier, card providers and merchants will endeavor to gain a competitive edge and reduce fraud-related costs and customer-frustration by acquiring the best technology. In fact, MasterCard acquired ElectraCard Services in May 2014 to bolster its risk management capabilities.

From a mobile payments perspective, we expect strategic acquirers to enhance their technology and product suites by acquiring leading-edge mobile payments, wallet, and commerce companies. Very recently, BBVA Compass acquired the mobile banking app Simple and MasterCard recently acquired the mobile wallet service C-Sam.

Based on these recent acquisitions, innovative mobile platforms appear to integrate well with the vast scale of financial institutions and card providers.

Conclusion

In conclusion, the switch to EMV standards poses substantial overhaul of current payments infrastructure, but can be seen as an investment in protection for both banks and consumers in the fight against credit and debit card fraud. As EMV-capable systems reduce in-person fraud, fraudsters will shift online, thus requiring merchants to adopt more advanced technology. The compatibility of EMV systems and mobile technology also creates significant opportunities for mobile payments, wallet, and commerce companies.

Footnotes

[1] The New York Times "For Target, the Breach Numbers Grow." January 2014. http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html

[2] QSR Magazine. "Are You Ready for EMV?"January 2013. http://www.qsrmagazine.com/exclusives/are-you-ready-emv

[3] Digital Transactions. Volume 11, Number 6. pp. 7-9. June 2014.

[4] TSYS. "EMV: Preparing for Changes to the Retail Payment Process." White Paper. 2013. http://www.tsys.com/acquiring/engage/white-papers/EMV-Preparing-for-Changes-to-the-Retail-Payment-Process.cfm

[5] First Data. "EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions." White Paper. 2011. http://www.firstdata.com/downloads/thought-leadership/EMV_US.pdf

[6] Smart Card Alliance Payments Council. "Card-Not-Present Fraud: A Primer on Trends and Authentication Processes." White Paper. 2014. http://www.smartcardalliance.org/resources/pdf/CNP-WP-FINAL-022114.pdf

[7] The Fraud Practice. "Credit Card Payments: Chargebacks & Fraud Liability." Accessed 2014. http://www.fraudpractice.com/fl-paychargeback.html

[8] American Express. "Card Not Present Fraud Webinar Transcript." Accessed 2014. https://www.americanexpress.com/us/content/merchant/pdf/knowledge-center/video-library/accessible-index/Card_Not_Present_Fraud_Webinar.pdf

[9] Forbes. "Mobile Payments: Why You Can't Live Without Them." June 2013. http://www.forbes.com/sites/groupthink/2013/06/18/mobile-payments-why-you-cant-live-without-them/

[10] Bank Innovation "It's Alive! NFC Is Back from the Dead." February 2014. http://www.bankinnovation.net/2014/02/its-alive-nfc-is-back-from-the-dead/