EMV & Payment Card Fraud

THE IMPACT OF EMV ON FRAUD TRENDS

Kelsey Neisen, Junior Research Associate
THE COPPER RIVER GROUP | FARGO, NORTH DAKOTA
August 17, 2015

About the Copper River Group

10 years and still going strong—The Copper River Group offers experience when you need it now.

The Copper River Group offers the experience and knowledge you're seeking to take your organization to the next level. The Copper River Group provides consulting and research services for independent community financial institutions. Our expertise is in vendor contract negotiations, regulatory compliance, and technology strategies.

The Copper River Group was established in 2005 in Fargo, ND. The company started with the mission to offer consulting services to community financial institutions. Since its inception, the Copper River Group has experienced a tremendous amount of growth. We provide services to financial institutions across the United States, and have worked internationally with banks in Canada and Ecuador.

Introduction: Development and Deployment of EMV

As new data breaches reach the media seemingly every week the push for stricter cyber security rules gains momentum. Consumers grow weary of receiving letters in the mail alerting them that their payment cards may be affected by another massive attack, or that their personal information was in an invaded database. Financial institutions tire of shelling out millions to pay for reissuing fees and fraud expenses. Retailers, the health industry, and insurance companies prove incident after incident their reluctance to increase their cyber security to protect consumers' information. No single all-encompassing solution exists to combat the threat of cyber criminals, but Europay-MasterCard-Visa (EMV) promises to significantly reduce payment card fraud in the United States.

In 1994 Europay, MasterCard, and Visa developed technology that utilized an encrypted chip embedded in a payment card. The chip functioned as a microprocessor that added another layer of authentication to card payment and made theft and counterfeiting of payment card data far more difficult for criminals.[1] Consumers use their EMV card by inserting it into an EMV enabled device face up and chip first. Much like traditional magnetic stripe cards, customers follow the prompts on the payment terminal and complete their transaction by either entering a PIN or signing on a receipt or terminal pad.[2] The only difference between EMV transactions and magnetic stripe transactions is the method in which the card is inserted and the level of security.

Currently, nearly every nation except the U.S. has switched to EMV payments. Most of the European countries converted to EMV in the early 2000s, and EMV now accounts for 96% of all payment card transactions. Canada, Latin America, and the Caribbean follow Europe with 83% EMV transactions. Africa, the Middle East, and Asia all come in at or above the 70% mark. The U.S., however, lags far behind at 0.03% of all payment card transactions EMV.[3] According to *Business Insider* estimates, the U.S. held 51% of global payment card fraud losses in 2013, and in 2012 the *Nilson Report* calculated 47% of global fraud with 23.5% of payment card volume.[4] With the rest of the world jumping on the EMV boat, the relatively 'easy pickings' and high payment card volume in the U.S. draws the eyes of cyber criminals to a ripe, poorly protected crop of potential victims.

The United Kingdom experienced rapidly rising fraud rates in the early 2000s and

[1] Smart Card Alliance. "EMV: FAQ," accessed February 25, 2015, http://www.smartcardalliance.org/publications-emv-faq/.
[2] Chase Paymentech. "FAQ: EMV Chip Card Technology," accessed February 25, 2015, https://www.chasepaymentech.com/faq_emv_chip_card_technology.html.
[3] EMVCo. "Worldwide EMV Deployment Statistics," accessed February 25, 2015, http://www.emvco.com/about_emvco.aspx?id=202.
[4] John Heggestuen. "The US Sees More Money Lost to Credit Card Fraud than the Rest of the World Combined," *Business Insider*, last modified March 5, 2014, accessed July 1, 2015, http://www.businessinsider.com/the-us-accounts-for-over-half-of-global-payment-card-fraud-sai-2014-3.

required a solution, so in January of 2004 EMV technology rolled out nationally. The price to purchase new terminals and software to process the updated cards caused concern for some retailers who believed the switch offered no financial benefit. To quell the critics, Visa and MasterCard announced in April 2005 that merchants who refused to switch to EMV by January 1, 2006 would assume the responsibility of paying for fraudulent charges on consumers' payment cards. Between 2004 and 2005, the U.K. witnessed a decrease of £60 million, or nearly $94 million, in payment card fraud losses. This drastic change led many other European countries to adopt EMV as well.[5]

Like the U.K., Canadians did not see a clear benefit to adopting EMV technology. They felt that their fraud rate remained relatively low despite the issues in other parts of the world, but when card issuers changed the message to the possibility of criminals aiming their malicious ministrations to Canada after the switch to EMV in Europe, more organizations accepted the conversion to EMV. Rollout started in 2008, and Visa expected to complete the transition by 2010. If merchants did not convert to EMV by March 31, 2011 the responsibility for fraudulent charges would fall on them. Between 2009 and 2010, Canada experienced a 16% decrease in card fraud.[6]

Between 2009 and 2010, Canada experienced a 16% decrease in card fraud.

EMV in the U.S.

The reluctance to switch to EMV in the U.S. stems from money. Like the U.K. and Canada, merchants feared costs to equip stores with new EMV compatible terminals would outweigh the amount of money lost to payment card fraud. As of 2010, the U.S. accumulated $2.9 trillion of payment card purchase volume, yet only 0.04% was lost to fraud, as compared to the U.K. who had a 0.18% rate. Instead of dishing out a one-time $8 million to complete EMV migration, U.S. merchants felt continuing to lose astronomical amounts of money every year to payment card fraud would be more favorable.[7] Interestingly enough, financial institutions, not merchants, bear most of the financial burden in fraud cases.

[5] Andrew Akers, Daniel Bogomoltz, Lisette De Later, Jonathan Mitchell, Shannon Mosier, and Brian Ramirez*. EMV Technology Commercialization in the UK and Canada (and the U.S.),* (Hannover: Tuck School of Business, November 11, 2011), 8-9, accessed February 26, 2015, http://faculty.tuck.dartmouth.edu/images/uploads/faculty/ron-adner/EMV_Technology_Commercialization.pdf.

[6] Andrew Akers, et al. *EMV Technology Commercialization*, 13-14.

[7] Andrew Akers, et al. *EMV Technology Commercialization*, 22-23.

It is an absurd notion to accept the rising cost of payment card fraud as a normal part of conducting business instead of implementing measures to reduce it. In 2012, $11.27 billion of the total global payment card purchase volume of $21.604 trillion was lost to fraud. Financial institutions paid for 63% of that sum, and merchants and acquirers only took responsibility for 37%. Card issuers lose money from counterfeit cards if the loss occurs at the point of sale system, while merchants and acquirers lose money in card-not-present situations, such as transactions performed over the phone or Internet. Additionally, the U.S. is the only region on the globe where counterfeit card fraud continues to grow.[8] The initial cost of the EMV conversion may stagger U.S. merchants at present, but after the October 2015 deadline they will find their future savings far diminish the worthy one-time cost.

It is an absurd notion to accept the rising cost of payment card fraud as a normal part of conducting business instead of implementing measures to reduce it.

Visa and MasterCard hold alternative motives for pushing EMV adoption in the U.S. Many predict quick, contactless transactions as the future of the payments system, and EMV technology serves as the perfect introduction for American consumers. Researchers at the Tuck School of Business at Dartmouth College believe that the push for EMV conversion has more to do with Visa and MasterCard building a stronger infrastructure for mobile payments than with decreasing fraud rates. They point to the fact that the conversion deadline for the U.S. is much shorter than in regions such as Canada or the U.K. Near-Field Communication enabled mobile devices reached the market in 2011, and Visa and MasterCard feared mobile payments would fail in the U.S. because merchants didn't have the terminals to support the new transactions as customers tried out the devices' new features.[9] Whatever the real reason for the U.S.'s reluctant adoption of EMV, the enormous loss of money and hassle it causes for consumers illustrate a clear need for change.

The Card Processing industry should re-define itself and lead with new and improved fraud fighting technology.
-Dan M. Fisher, President & CEO, The Copper River Group

[8] "Global Card Fraud Losses Reach $11.27 Billion," *The Nilson Report*, Issue 1023, August 2013, 6.
[9] Andrew Akers, et al. *EMV Technology Commercialization*, 25-26.

EMV payment cards may nearly eliminate card-present (CP) fraud—when the card holder uses the card in a physical store location—but criminals prove their adaptability by devising other methods to grasp the information they require. In the U.K., card-not-present (CNP) fraud, such as transactions on the Internet or over the phone, account for 62% of payment card fraud. CNP and cross-border fraud reached their peak in 2008.[10] In fact, in the first three years after the U.K. switched to EMV, CNP fraud rose 79%, and Canada's CNP fraud rate skyrocketed 133%. In 2014, CNP fraud accounted for 45% of all payment card fraud in the U.S.[11]As the U.S. continues to move toward EMV conversion they can expect that number to rise dramatically as criminals explore other avenues of compromising consumers' payment card data. The U.S. knows what to expect, so measures to curb CNP fraud must be implemented at once.

Tokenization may prove to be the answer to alarming rise of CNP fraud after EMV conversion. Tokenization replaces the primary account number of payment cards and replaces it with a 'token.' The token is useless by itself and typically looks like a string of nonsensical jibberish. They can be mathematically created with a cryptographic function, or randomly generated, but either way they must be useless to criminals if stolen and never reveal payment card details if the database is compromised.[12] Implementation proves difficult, however, due to lack of standardization. A type of token that works at one retailer may not work with another.[13] Consumers will be unlikely to adopt tokenization if only a handful of the retailers they regularly visit possess the necessary equipment to process token transactions, and they do not want to have multiple payment apps on their mobile devices.

These measures helped reduce CNP fraud in the U.K. by 19% in 2009.

MasterCard and Visa developed a method called 3D Secure to increase security for CNP transactions. 3D stands for 3 Domain Server and involves the merchant, the acquiring bank, and Visa or MasterCard. The companies' products are called Verified by Visa and MasterCard SecureCode, enrolled cardholders initiate the process by simply clicking the 'buy' button

[10] Douglas King. "Chip-and-Pin: Success and Challenges in Reducing Fraud," *Retail Payments Risk Forum,* (Atlanta: Federal Reserve Bank of Atlanta, January 2012), 8.

[11] Tony Mecia. "Online fraud may surge after EMV chip card rollout," *CreditCards.com*, last modified November 19, 2014, accessed July 6, 2015, http://www.creditcards.com/credit-card-news/online-fraud-surge-emv-1273.php.

[12] Scoping SIG, Tokenization Taskforce, PCI Security Standards Council. *Information Supplement: PCI DSS Tokenization Guidelines*, August 2011, accessed February 27, 2015, https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf.

[13] Eduard Kovacs. "Tokenization: Benefits and Challenges for Securing Transaction Data," *Security Week*, last modified November 4, 2014, accessed July 6, 2015, http://www.securityweek.com/tokenization-benefits-and-challenges-securing-transaction-data.

on supported merchant websites. If a cardholder is not enrolled, the merchant has the option to discontinue the transaction. The cardholder will be directed to MasterCard or Visa's 3DS webpage where they will enter their unique password. If the password is not matched, the cardholder is presumed a fraud and the transaction will be terminated.[14] These measures helped reduce CNP fraud in the U.K. by 19% in 2009.[15] Unfortunately, merchants find 3D Secure software expensive in addition to monthly fees and transaction fees, so few merchants possess the technology.[16] 3D Secure offers additional protection to merchants by shifting loss liability to the issuing bank instead of forcing the retailer to take the chargeback, yet the technology's popularity remains minimal.[17]

Micro-computers built right into the payment card are another technology Visa and MasterCard pursue. Emue Technologies, a company created by security and technology specialists in Australia, developed a payment card containing a display, microprocessor, and keypad specifically designed to combat CNP fraud. The cardholder begins the Visa Emue Card, or Visa CodeSure, verification process by pushing the Verified by Visa button on the card's keypad. When prompted, the cardholder enters their PIN on the keypad, and a one-time passcode will appear on the card's display screen. Cardholders use the passcode to authenticate their online transactions.[18] Currently, little word of Visa CodeSure has reached American shores, but in late 2011 Visa released CodeSure from beta testing and prepared to deliver the technology to the U.K.[19]

Card Processors generate significant revenue from good and fraudulent transactions. Particularly from fraud detection tools, case generation, and card re-issue events, where is the incentive for the processor to significantly reduce fraud?
-Dan M. Fisher, President & CEO, The Copper River Group

Similar to Visa CodeSure, the MasterCard Display Card serves as a security token card. MasterCard and NagraID Security of Switzerland collaborated on the project

[14] Datacash. "3D Secure," accessed February 26, 2015, http://www.datacash.com/mcdatacash/implementation_guides/3D-Secure.html.
[15] Miles Brignall. "Visa CodeSure card to combat fraud," *The Guardian*, last modified July 9, 2010, accessed July 6, 2015, http://www.theguardian.com/money/2010/jul/10/visa-codesure-card-combat-fraud.
[16]Andrew Akers, et al. *EMV Technology Commercialization*, 20.
[17] "Free Verified By Visa/MasterCard SecureCode," *CDG Commerce*, accessed July 6, 2015, http://www.cdgcommerce.com/vbv_msc.
[18] Emue. "Visa Europe makes investment in Emue Technologies," press release November 17, 2009, accessed February 26, 2015, http://www.emue.com/sites/default/files/pdf/Emue%20Technologies%20-%20Press%20Release%20-%20Visa%20Europe%20Investment%20-%2017%20Nov%202009.pdf.
[19] Eric Doyle. "Visa Launches CodeSure Matrix Display Cards," *TechWeek Europe*, last modified October 17, 2011, accessed July 6, 2015, http://www.techweekeurope.co.uk/workspace/visa-launches-codesure-matrix-display-cards-42454.

and launched the Display Card 2010.[20] The first deployment occurred in Taiwan with Bank SinoPac in October of 2010, and later Turkish bank TEB in November 2011 with a multi-function display card. The collaboration with Standard Charter Bank Singapore in 2012 proved the largest deployment of Display Card.[21] Like the CodeSure card, the MasterCard Display Card has yet to appear in the U.S.

> **The business model from the card processor standpoint needs to change to a performance based model that compensates based on fraud fighting effectiveness.**
> **-Dan M. Fisher, President & CEO, The Copper River Group**

Criminals Attack Personally Identifiable Information

Despite the new technologies and consumer tools that promise to curb and shrink the payment card fraud epidemic, criminals will find more innovative methods to steal data with which they can turn a profit. As payment cards become more difficult targets, the health industry and government agencies will see a sharp increase in the frequency and magnitude of their data breaches. In 2014 alone, roughly 59,313,100 records of payment card information were exposed by 35 data breaches within the retail industry, as opposed to approximately 4,536,981 records stolen by criminals from 11 data breaches in the health industry. In just half a year and with only 6 data breaches, hackers stole 91,151,626 records from the health industry, including health insurers, hospitals, dental offices, and clinics. In 2015, retailers and merchants reported 8 hacks with an unknown number of records compromised.[22] This behavior indicates a shift from payment card information, which can have a short life for criminals, to personally identifiable

> **As payment cards become more difficult targets, the health industry and government agencies will see a sharp increase in the frequency and magnitude of their data breaches.**

[20] MasterCard. “MasterCard Introduces Next Generation ‘Display Card’ Technology, a First for Singapore,” press release November 7, 2012, accessed February 26, 2015, http://newsroom.mastercard.com/press-releases/mastercard-introduces-next-generation-display-card-technology-a-first-for-singapore/.

[21] Sarah Jacobsson Purewal. “MasterCard shows ‘Display Cards’ with LCD screen and PIN,” *TechHive*, last modified November 9, 2015, accessed July 6, 2015, http://www.techhive.com/article/2013727/mastercard-shows-display-cards-with-lcd-screen-and-pin.html.

[22] Privacy Rights Clearinghouse. “Chronology of Data Breaches,” accessed July 10, 2015, http://www.privacyrights.org/data-breach.

information, which can be used to create fake identities and run intricate health fraud schemes over extended periods of time.

Not even the United States government remains safe from determined hackers. The largest government hack in 2015, the Office of Personal Management in Washington, D.C., hackers exposed 21.5 million records of individuals who currently work, previously worked, or attempted to get a job with the government. To date, that attack is the largest against U.S. government networks.[23] Some think the hackers' goal is to spy on the United States, while others believe they're selling the personal information on the Black Market. For criminals, payment card information is an outdated product. As fraud controls increase in ingenuity and complexity, hackers will turn to easier targets.

This behavior indicates a shift from payment card information, which can have a short life for criminals, to personally identifiable information, which can be used to create fake identities and run intricate health fraud schemes over extended periods of time.

Criminals find personally identifiable information more valuable than payment card information, and recently this data proved even easier to access. Personally identifiable information (PII) can be sold for hundreds of dollars, as compared with the $1 to $20 for payment card information. Additionally, the healthcare industry holds a notorious record for the least adequate cyber security measures.[24] In April of 2014, the FBI warned the health industry that their cybersecurity measures were sub-par, and they were warned again in August of 2014 that hackers were likely to target them for PII.[25] Despite the repeated warnings, the health industry continues to overlook important security failures and neglect implementing proper measures to keep their patients' data safe.

[23] Julie Hirschfeld Davis. "Hacking of Government Computers Exposed 21.5 Million People," *The New York Times*, last modified July 9, 2015, accessed July 10, 2015, http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0.

[24] Tim Greene. "Anthem hack: Personal data stolen sells for 10x price of stolen credit card numbers," *NetworkWorld*, last modified February 6, 2015, accessed July 13, 2015, http://www.networkworld.com/article/2880366/security0/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[25] Jim Finkle. "FBI Warns healthcare firms they are targeted by hackers," *Reuters*, last modified August 20, 2014, accessed July 20, 2015, http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

The health industry continues to make critical mistakes in their cyber security procedures. Although Anthem encrypted outbound information, they did not encrypt data stored on their computers. The failure allowed hackers to steal 80 million records laden with PII and personal health records in February 2015.[26] Even the smallest devices, such as tablets, smartphones, and even printers, offer a gateway to hackers provided they are connected to the organization's network. More than 60% of data breaches in the health industry originated from an end-point device. Employees bringing their own mobile devices to work and using them to access the organization's network further weakens cybersecurity, because personal, unregulated mobile devices often prove unsecure.[27] Additionally, the Health Insurance Portability and Accountability Act (HIPAA) does little to protect patients from theft of their electronic medical files. Although HIPPA requires the health industry to implement cybersecurity measures to protect their patients' data, it is clear their efforts are failing.[28] The growing trend for criminals is stealing PII, and if organizations entrusted with this information neglect to keep it safe, the implications could be catastrophic.

The growing trend for criminals is stealing PII, and if organizations entrusted with this information neglect to keep it safe, the implications could be catastrophic.

The Impact of Identity Theft

Victims of identity theft experience an immense amount of frustration as they erase debts they never incurred and fend off collection agencies. Out of pocket financial losses can amount to $10,000 or more as victims attain legal help to prove their

Out of pocket financial losses can amount to $10,000 or more as victims attain legal help to prove their own identity.

[26] Reed Abelson and Matthew Goldstein. "Anthem Hacking Points to Security Vulnerability of Health Care Industry," *The New York Times*, last modified February 5, 2015, accessed July 20, 2015, http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=0.
[27] Jaspreet Singh. "Endpoint Devices & the Battle for Data Security," *Healthcare Global*, last modified June 20, 2013, accessed July 22, 2015, http://www.healthcareglobal.com/tech/1140/The-Battle-For-Data-Security.
[28] Leon Rodriguez. "Privacy, Security, and Electronic Health Records," *HealthIT Buzz*, last modified December 12, 2011, accessed July 30, 2015, http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/privacy-security-electronic-health-records/.

own identity.[29] The cost of identity theft does not stop at the victim, however. Victims of identity theft maintain the right to order debt collectors from contacting them after they prove their identity and file the correct reports. In most states, victims are not responsible for any fraudulent charges under new accounts in their name opened without their permission.[30] Businesses who allowed the criminal to apply for credit or services eat those fraudulent charges, because they have no real person to contact for the collection of their debts.

Identity theft does not stop at fraudulent applications for credit and services, but encompasses an entirely new type of scheme. In June of 2015, the IRS announced that criminals gained unauthorized access to 100,000 tax accounts through their "Get Transcript" application. The criminals used PII apparently stolen from another source, such as one of the many recent data breaches like Anthem. They correctly answered questions about Social Security numbers, birth dates, and street addresses in the multi-step authentication process, as well as personal questions only the taxpayer would know.[31] The IRS attack demonstrates the chaos criminals can generate wielding PII, and raises questions about the security of organizations' authentication processes.

Consumers must take control of their financial records and utilize the tools their financial institutions offer them to monitor their accounts.

Consumers must take control of their financial records and utilize the tools their financial institutions offer them to monitor their accounts. It is important that consumers keep their contact information, such as phone numbers and street addresses, current so their financial institutions can reach them if they detect fraudulent activity on their card. With the rising rate of PII theft, consumers should also consider purchasing a credit monitoring service such as LifeLock, or using a free application such as Credit Karma. These services can help consumers detect identity theft before a criminal irrevocably damages their victim's credit report. Most financial institutions and credit monitoring services also offer text message or e-mail alerts if a certain amount of money is withdrawn from their account or if a change occurs on their credit report. Card fraud and identity theft can happen quickly and without the victim's knowledge, so it is important for consumers to take advantage of credit and account monitoring tools that alert them to changes as quickly as criminals can open fraudulent accounts in their victims' names.

[29] Erika Harrell and Lynn Langton. "Victims of Identity Theft, 2012," *U.S. Department of Justice, Bureau of Justice Statistics*, last modified December 2013, accessed July 23, 2015, http://www.bjs.gov/content/pub/pdf/vit12.pdf.

[30] Federal Trade Commission. "Know Your Rights," *IdentityTheft.gov*, accessed July 23, 2015, https://www.identitytheft.gov/know-your-rights.html.

[31] Internal Revenue Services. "IRS Statement on the "Get Transcript" Application," *IRS*, last modified June 2, 2015, accessed July 23, 2015, http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application.

Conclusion

Like the businesses they attack, cyber criminals and identity thieves adapt to the changing environment to meet their needs. Organizations must identify the new avenues criminals will take, such as CNP fraud and theft of PII, so they can better protect their customers. Cyber breaches and identity theft are crimes that behave like shockwaves through the economy. No person or entity remains exempt from the financial toll no matter how far from the impact they stand.