Aite PARTNER. ADVISOR. CATALYST.

IMPACT NOTE

MAY 2016

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

EMV: Issuance Trajectory and Impact on Account Takeover and CNP

Sponsored by:

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

The United States has finally joined the rest of the G-20 countries in upgrading to the EMV standard, though the path has certainly been a rocky one. With the largest and most fragmented card market and no government support in the education process, the U.S. transition promised to be challenging from the outset. The Durbin amendment further complicated matters with its debit-routing provisions, delaying the debit upgrade for many merchants and financial institutions (FIs), since it took the industry more than a year to come up with a technical Durbin-compliant solution. As a result of this as well as bottlenecks in the certification process, many merchants have not yet completed their reterminalization process—an average of only 20% of credit card transactions and 10% of debit transactions are chip-on-chip as of March 2016.

While EMV gradually works its way into the fabric of U.S. payments, financial fraud continues to rapidly increase. Account takeover (ATO), card-not-present (CNP) fraud, and application fraud are all rapidly rising, fueled by reams of data breaches that have given criminals vast stores of consumer data. In 2015 alone, criminals compromised more than 477 million records containing online credentials, personally identifiable information (PII), and stolen card data.[1] Lessons learned from countries that preceded the United States in upgrading to EMV indicate that as the U.S. migration progresses, dwindling counterfeit card opportunity will further magnify the increases in other forms of fraud.

This Impact Note is sponsored by iovation, which wanted to investigate the state of the U.S. EMV migration and the associated account takeover, CNP fraud, and application fraud trends. The research will help FI executives benchmark their EMV progress against their peers' and better understand the rapidly shifting fraud landscape.

METHODOLOGY

To understand the current state and trajectory of the U.S. EMV migration as well as the concurrent fraud shifts, Aite Group interviewed 16 large U.S. issuers, four issuing processors, and two payment networks between February and April 2016. Collectively, the interviewees represent 73% of the credit card issuing market and 69% of the debit card issuing market.

1. Breach Level Index, accessed on February 26, 2016, http://breachlevelindex.com. Criminal compromises include data breaches, skimming, and theft by insiders.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

EMV: THE STATE OF U.S. MIGRATION

While merchant reterminalization continues to lag, large U.S. issuers have moved quickly to get chip cards in the hands of consumers. Table A shows the percentage of debit and credit card portfolios that have been reissued for the interviewees as of Q1 2016. Banks are prioritizing reissuance for active cardholders and high-net-worth individuals—the cardholders that represent the most financial exposure for a bank. For example, while Bank A has reissued 40% of its debit cards and 50% of its credit cards thus far, those cardholders collectively represent 70% of the FI's total debit card spend and 80% of credit card spend. Similarly, while Bank H has only reissued 30% of its credit cards, that represents 75% of total spend. Notably, one of the large FIs interviewed currently has no plans to upgrade its cards to be chip-capable, although its circumstances are somewhat unique; this FI has outsourced its fraud management, including most of the fraud liability, to its processor.

As was the case in many countries that preceded the United States in migrating to EMV, criminals' counterfeit fraud activity has escalated during the transition to chip. Criminals realize that their window for perpetrating counterfeit card fraud in the United States is rapidly closing, so they are working through their vast stocks of compromised cards. Gift cards remain one of fraudsters' favorite purchases, thanks to the ease with which the counterfeit card can be turned into an untraceable, easily monetized asset.

Table A also shows the directional impact of EMV on net and gross counterfeit card fraud thus far. Net fraud is the losses absorbed by the issuer after it has exercised its chargeback rights, while gross fraud is the total amount of counterfeit fraud perpetrated by criminals. Net fraud is down for many issuers year over year. Part of this is attributable to the fact that a year ago issuers were dealing with the fallout from major breaches of companies such as Home Depot, which resulted in significant counterfeit fraud losses, but another significant driver of the net fraud decline is the fact that issuers can now charge counterfeit fraud losses back to merchants that have not yet upgraded to EMV-capable terminals.

Table A: Chip Card Issuance and Counterfeit Fraud Impact

	Issuer size	Percentage of debit cards reissued	Percentage of credit cards reissued	Net counterfeit fraud direction	Gross counterfeit fraud direction
Bank A	Top 10	40%	50%	↓	↑
Bank B	Top 10	Unknown	70%	↓	↑
Bank C	Top 10	65%	90%	↓	↑
Bank D	Top 10	0%	100%	↓	↓
Bank E	Top 10	N/A	100%	↓	↓
Bank F	11 to 20	12%	85%	↓	↓
Bank G	11 to 20	20%	53%	↑	↑
Bank H	11 to 20	50%	30%	↓	↓

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Bank I	11 to 20	80%	100%	↓	↓
Bank J	11 to 20	0%	50%	↓	↓
Bank K	21 to 30	65%	N/A	↓	↓
Bank L	21 to 30	41%	6%	↔	↑
Bank M	31 to 40	90%	20%	↑	↑
Bank N	31 to 40	0%	0%	↑	↑
Bank O	41 to 50	50%	50%	↓	↑

Source: Aite Group interviews with 20 large issuers and processors, February to April 2016

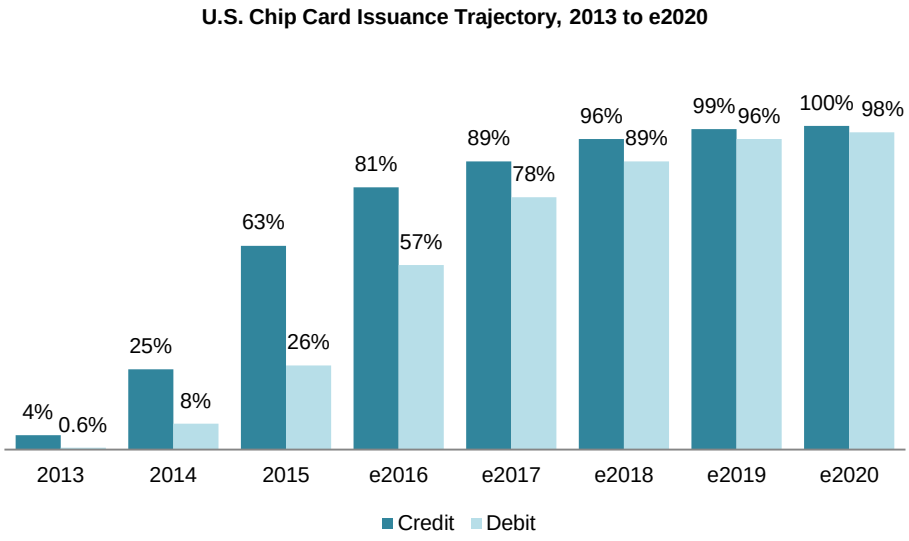
Issuers with at least 50% of their portfolio reissued report an average of a 25% year-over-year decrease in net counterfeit fraud. One of the issuers that has reissued 100% of its portfolio is down a whopping 65% year over year and expects counterfeit fraud losses to be down 80% year over year by the end of 2016. The only significant source of counterfeit losses this issuer is still absorbing are purchases at the gas pump (which don't see a shift in liability until 2017) and charges that are less than US$25 (this issuer deems the labor needed to process the chargeback is more costly than the benefit).

The numbers also clearly show the extent to which criminals do their homework. Many of the banks that have been more aggressive in reissuing their cards are seeing declines not only in net fraud but also in gross fraud. All three of the issuers that have reissued their entire credit card portfolio report "significant decreases" in gross fraud as well. This is a stark contrast to other issuers who are further behind in the reissuance process, the majority of which report continued increases in their gross fraud rate. This clearly indicates that the criminals are aware that compromised cards from predominantly chip-capable FIs are going to be more difficult to monetize, so they are focusing their counterfeit activity on issuers that have fewer chip cards in the market.

Figure 1 and Figure 2 show the trajectory for upgrading the balance of the U.S. credit and debit card portfolios. By the end of 2016, 81% of credit cards and 57% of debit cards will be EMV-capable. The approach to completing reissuance varies among the FIs interviewed. Many FIs performed a forced reissuance for their highest spending and most active clients, and once those are complete will reissue the balance of their portfolio at the card's natural expiry date. Other FIs are performing a mass reissuance of their entire portfolio, with the goal of having the entire process complete in 2016 or early 2017. Small FIs continue to lag, and some will trail into 2017 and beyond to complete their conversion.

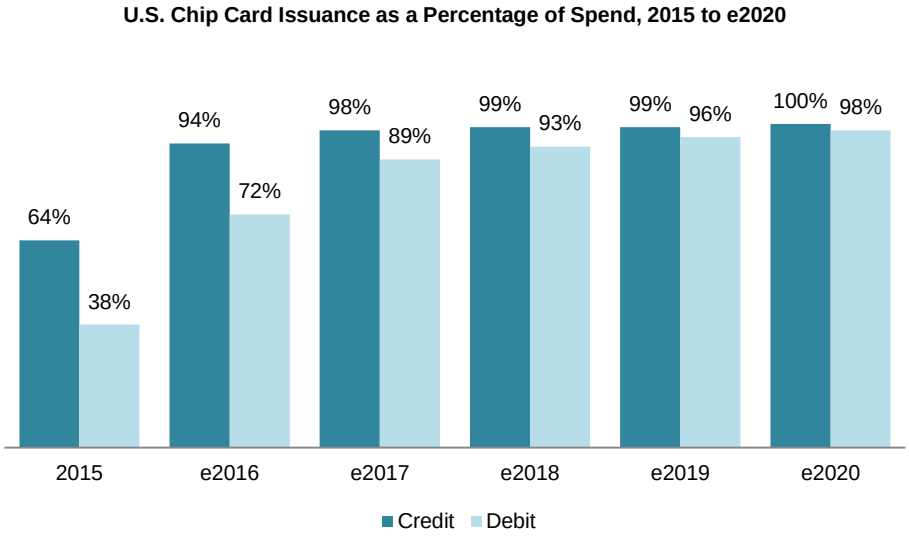
101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 1: Chip Card Issuance Trajectory



Source: Aite Group interviews with 20 large issuers and processors, February to April 2016

Figure 2: Chip Card Issuance as Percentage of Spend



Source: Aite Group interviews with 20 large issuers and processors, February to April 2016

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

To minimize the impact on customers' recurring billing arrangements, almost all of the issuers interviewed are issuing cards with the same Personal Account Number (PAN) and a new expiration date, and processors report that the majority of smaller FIs are following suit. Only two of the issuers interviewed are issuing a significant portion of their portfolio with new PANs. One of the issuers acquired another bank in 2015, so the new PANs are part of incorporating the acquired bank's portfolio. Another issuer began its debit reissuance with the same PAN but saw fraudsters exploiting gaps in its defenses, so made the decision to reissue the balance of its debit portfolio with new PANs.

In a similar vein, only one of the 16 issuers interviewed is issuing dual-interface cards, which are capable of contactless transaction; the rest of the issuers are issuing contact-chip only. Among the processors, two report that none of their clients are issuing contactless cards, one states that around 15% of the cards issued by its issuing clients are contactless, and the fourth says the vast majority of its U.S. clients are issuing contact-chip cards, with just two clients beginning contactless pilots. Many of the issuers say that their contactless strategy continues to focus on the mobile device; others cite the higher cost of chip cards as a deterrent. For a small issuer, contactless cards cost an extra US$2 per card, while midsize issuers will pay half that—an extra US$1 per contactless card. Although there have been early complaints about the length of time an EMV transaction takes at the point of sale, none of the issuers interviewed have near- or mid-term plans to transition to contactless.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

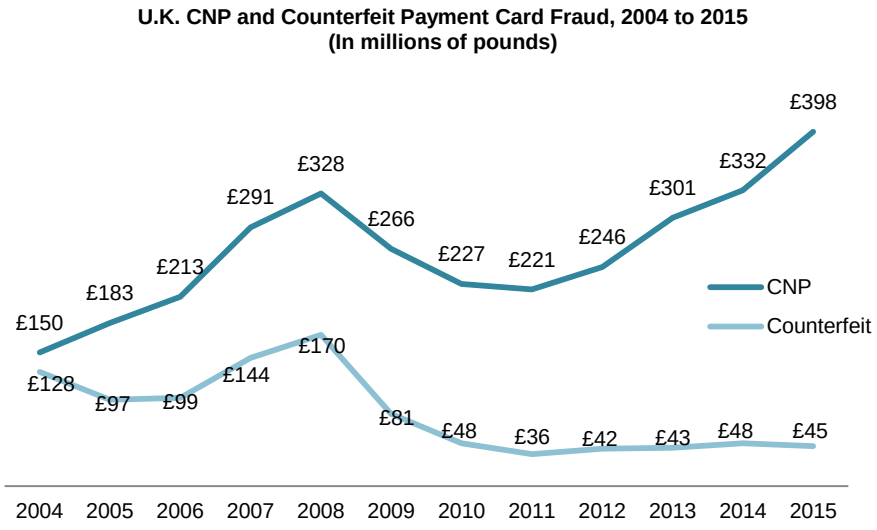
LESSONS LEARNED FROM OTHER COUNTRIES

As the United States moves to EMV, fraud rings will not sit idle while their revenue from counterfeit card fraud gradually melts away. Instead, they will shift their tactics to other forms of fraud. Plenty of precedent from other countries can help educate the U.S. industry about the types of fraud that will see an uptick post-EMV: CNP, ATO, and application fraud.

CNP FRAUD

The U.K. was one of the first countries to move to EMV, and the technology has been very effective at reducing counterfeit card fraud there. After 2015, the vast majority of the GBP45 million in counterfeit card fraud remaining was cross-border (i.e., criminals make counterfeit cards using compromised U.K. cardholder data and use them in countries that don't yet have uniform support for EMV, such as the United States). With declining counterfeit fraud in the wake of its February 2006 liability shift, the U.K. experienced steadily rising CNP fraud. Development of more advanced fraud analytics by issuers and merchants, as well as increased use of 3-D Secure technology helped to rein in the rising problem.[2] Since 2012, however, CNP fraud has resumed its steady rise (Figure 3).

Figure 3: U.K. CNP and Counterfeit Payment Card Fraud



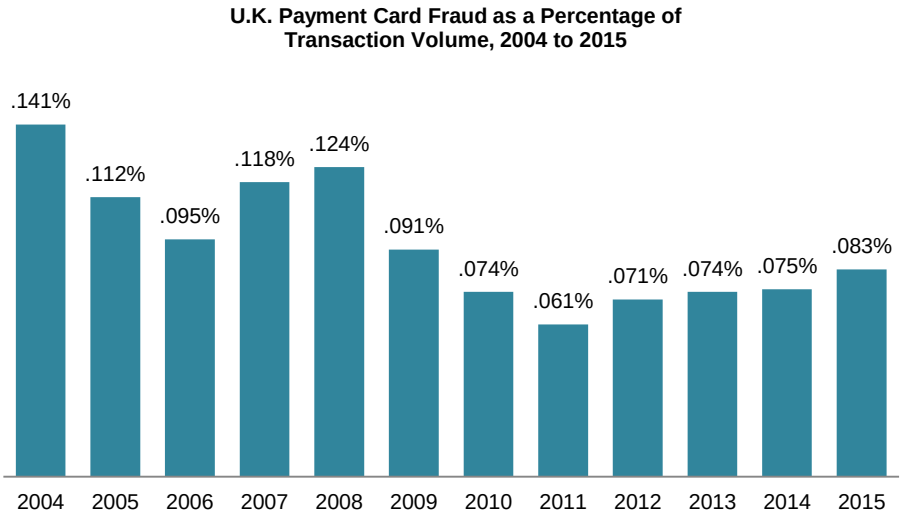
Source: Financial Fraud Action UK

2. See Aite Group's report *Not Your Father's 3-D Secure: Addressing the Rising Tide of CNP Fraud*, February 2016.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Part of this is due to criminals making adjustments of their own to evade detection, such as focusing on cross-border e-commerce as an attack vector—fully 25% of the U.K. CNP fraud is attributable to cross-border e-commerce transactions. A good portion of the rise is also attributable to e-commerce's rapid growth. U.K. e-commerce grew 21% year over year from 2014 to 2015, while e-commerce card fraud grew 19% during the same period.[3] The parallel growth rates of fraud and commerce are further substantiated by the fact that fraud as a percentage of total transaction volume has held fairly steady for the past few years (Figure 4).

Figure 4: U.K. Payment Card Fraud as a Percentage of Transaction Volume



Source: Financial Fraud Action UK

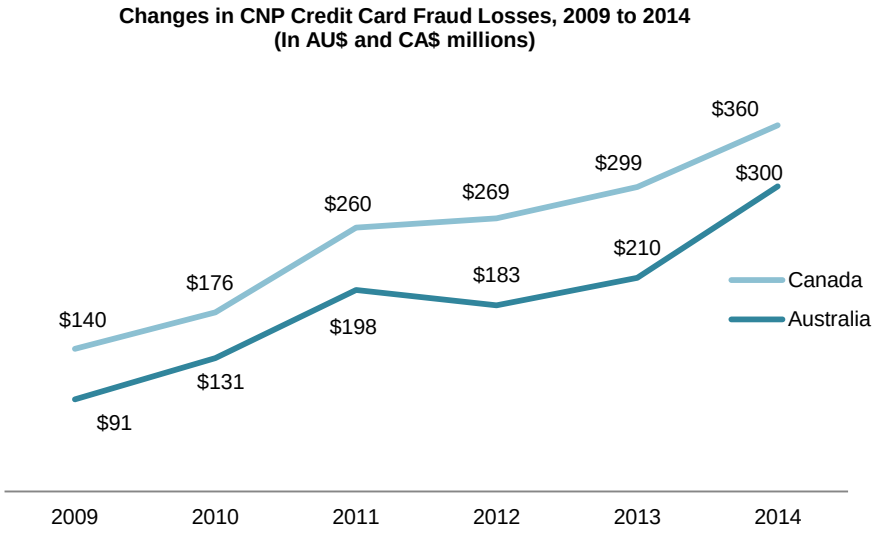
CNP fraud losses spiked in the wake of Canada's 2011 liability shift as well as in Australia, where the liability shift took place in April 2012 for MasterCard and April 2013 for Visa (Figure 5). In Australia, the pace of CNP fraud growth outpaced that of e-commerce sales; Australia's e-commerce fraud losses increased 30% from 2013 to 2014, while its aggregate e-commerce sales growth was only 9% for the same period.[4]

3. "Year-end 2015 Fraud Update: Payment Cards, Remote Banking and Cheque," Financial Fraud Action UK, accessed on March 21, 2016, http://www.financialfraudaction.org.uk/cms/assets/1/downloads-7-3085-2015-year-end-fraud-update-report.pdf.

4. NAB Online Retail Sales Index, accessed on January 12, 2016, http://business.nab.com.au/wp-content/uploads/2015/03/NAB-Online-Retail-Sales-Index_in-depth-report-January-20151.pdf.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 5: Post-EMV CNP Fraud in Australia and Canada



Source: Canadian Bankers Association, Australian Payments Clearing Association

ACCOUNT TAKEOVER

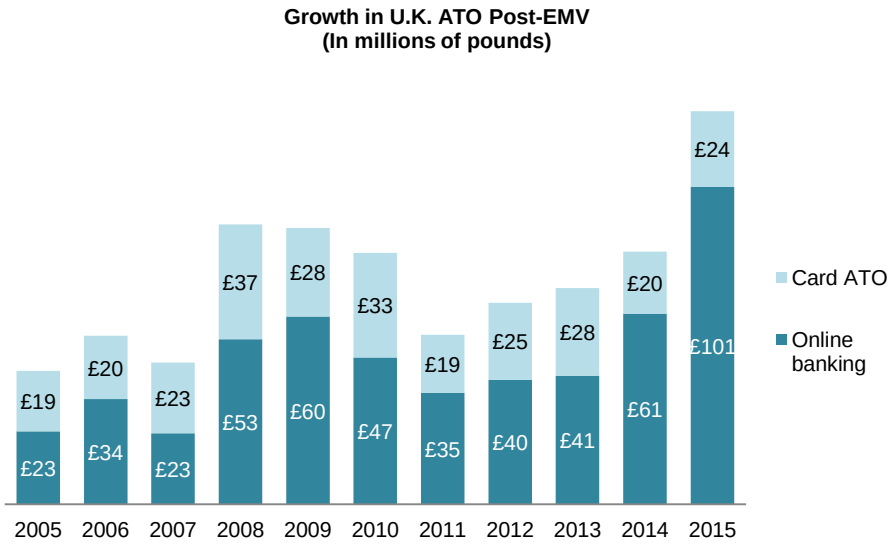
CNP transactions are not the only area of intensifying attacks post-EMV. Account takeover is another key area of fraud migration, as criminals leverage the large supply of compromised login credentials and PII at their disposal to take over existing accounts. ATO more than tripled in the wake of the U.K. EMV migration, from GBP42 million in 2005 to GBP125 million in 2015 (Figure 6). The U.K. FIs track ATO in two discrete categories, defined as follows:

- **Card ATO:** In this scenario, criminals gather information about the intended victim and then contact the FI, masquerading as the genuine cardholder. The criminals then arrange for funds to be transferred out of the account or change the address on the account and request replacement cards.
- **Online banking ATO:** This is the act of illicitly accessing and/or transferring funds from an individual's online banking account for the purpose of financial gain.

Escalating attacks combining phishing, social engineering, and sophisticated malware are to blame for the continued growth in U.K. ATO losses.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 6: Post-EMV ATO in the U.K.



Source: Financial Fraud Action UK

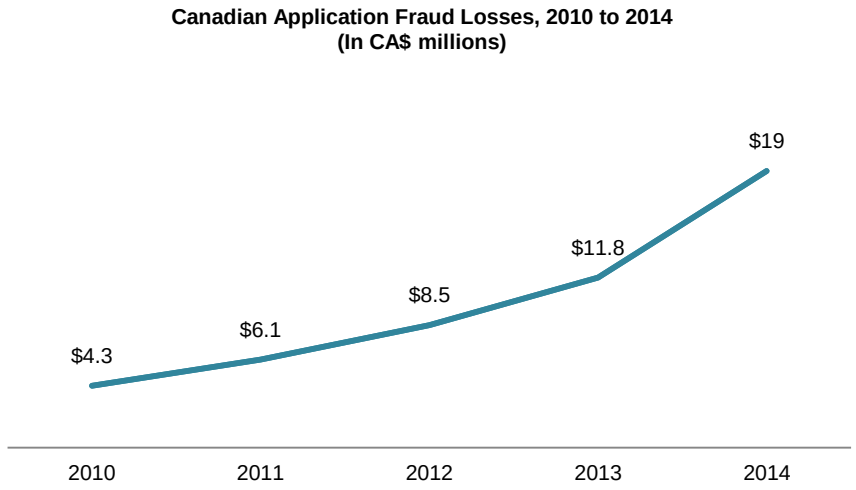
While Australia and Canada do not track account takeover at the macro level, Aite Group interviewed two large Canadian FIs that also saw a significant increase in their account takeover losses in the wake of Canada's switch to chip.

APPLICATION FRAUD

Application fraud is another area to which criminals shift their activity post-EMV, and Canada's experience is a prime example. Fraudsters could no longer buy stolen card data on the underweb and use it to make counterfeit cards, so they switched to application fraud to get cards of their own using stolen and synthetic identities. As Canadian counterfeit card fraud sharply declined, FIs' application fraud losses increased nearly 500% in the wake of its EMV migration (Figure 7).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 7: Canada's Increasing Application Fraud Losses



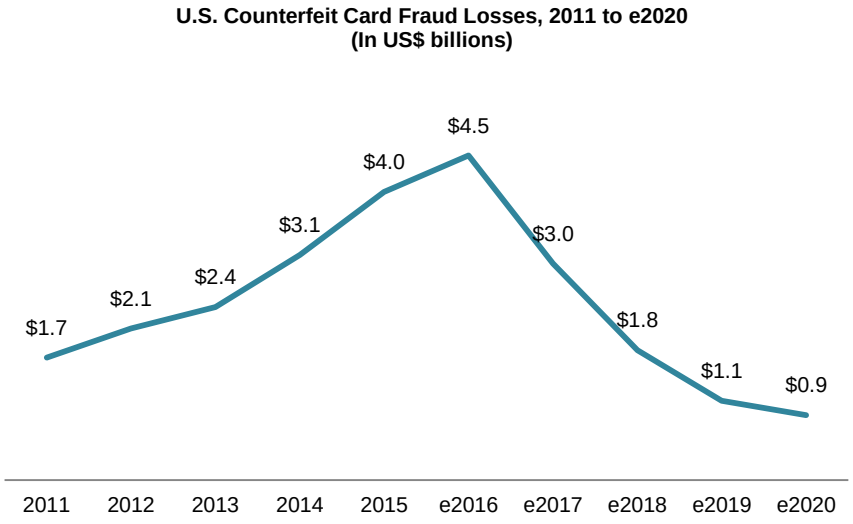
Source: Canadian Bankers Association

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

POST-EMV FRAUD TRENDS

As the United States moves to EMV, it will see similar fraud migrations. As more than US$4 billion in counterfeit fraud gradually disappears, criminals will turn instead to CNP fraud, ATO, and application fraud. Similar to many other countries, gross counterfeit fraud is increasing in the year following the EMV transition, as criminals burn through their stocks of compromised card data before the opportunity to leverage this data disappears. Counterfeit fraud opportunity will rapidly diminish as more merchants become EMV-capable, however, falling from a high of US$4.5 billion in 2016 to less than US$1 billion in 2020 (Figure 8). Cross-border counterfeit fraud will not be as significant an issue for U.S. issuers as it was for issuers in the U.K. and Canada, since there will be relatively few non-EMV card markets of any size, and U.S. issuers' analytics will be tuned to spot emergent cross-border fraud patterns.

Figure 8: U.S. Counterfeit Card Fraud



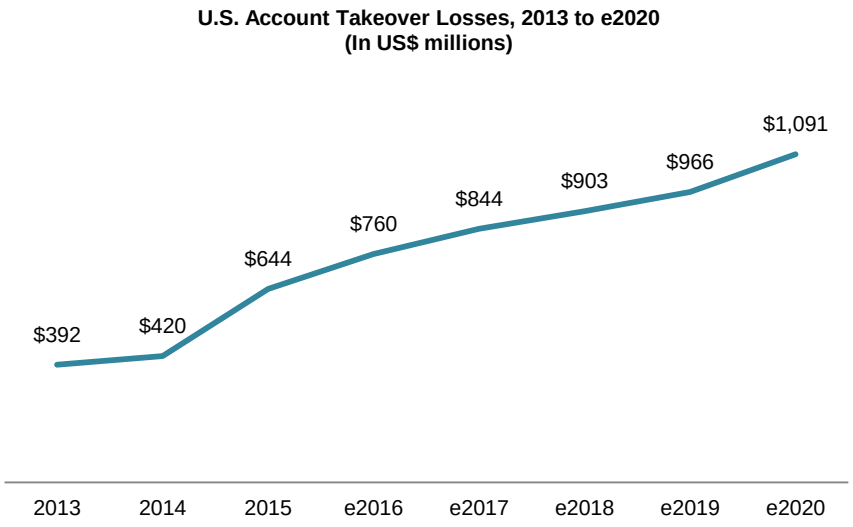
Source: Aite Group

ACCOUNT TAKEOVER

Account takeover manifests in many ways, from phishing emails designed to compromise user credentials to malware to social engineering attacks on the FI's call center—and often more than one concurrently. After a brief plateau in FIs' ATO losses from 2013 to 2014, the majority of the FIs interviewed are once again experiencing significant increases in ATO. Two of the FIs interviewed report 100% increases in ATO from 2014 to 2015, while another two FIs state that their ATO increased 200% over the same time period. As a result, Aite Group expects ATO losses to increase from US$644 million in 2015 to over US$1 billion by 2020 (Figure 9).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 9: U.S. FI Account Takeover Fraud



Source: Aite Group

Attack vectors vary somewhat by FI. Criminals are actively probing the defenses of FIs, looking for the soft underbelly. Some FIs report significant pain emanating from the contact center, where criminals are successfully calling in to place travel alerts via agents or interactive voice response (IVR), resetting PINs, verifying suspicious activity, and changing addresses. Other FIs are seeing more pain in the online environment, with brute-force attacks on credentials or address changes closely followed by large CNP transactions. Still other FIs are seeing increases in ATO equally across all channels.

APPLICATION FRAUD

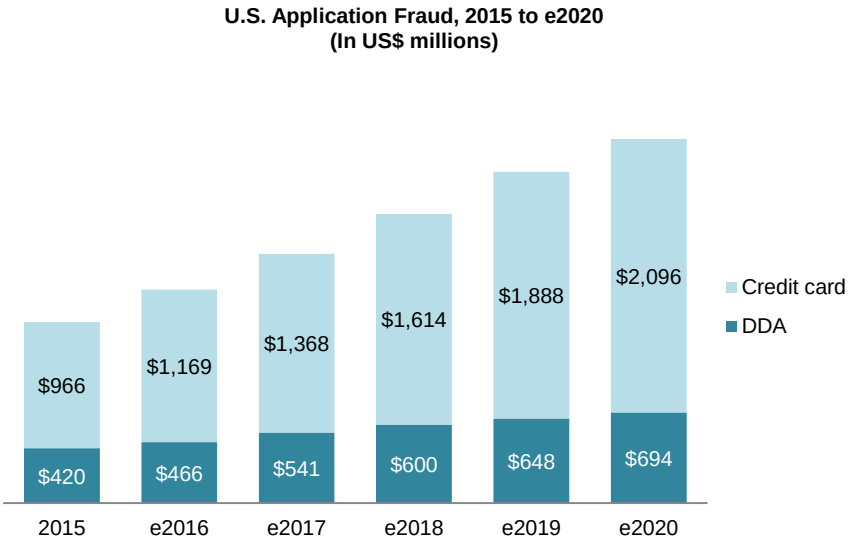
Concurrent with the U.S. shift to EMV, breaches have made consumers' PII readily available for organized crime, while larger FIs are making a concerted effort to expand their footprint and increase the proportion of their onboarding activity that takes place via the higher-risk digital channels. All of these factors will contribute to a continued uptick in application fraud for U.S. FIs. A number of the FIs interviewed report sharp increases in application fraud losses, with five of the FIs seeing over 100% spikes year over year.

U.S. demand deposit account (DDA) application fraud losses will total US$466 million in 2016 and will grow to US$694 million by 2020. The official application fraud numbers that credit card issuers report to the payment networks amount to around 2% of total credit card fraud, but the problem is substantially bigger than that, since first-party fraud (i.e., identity fraud without a victim) is often misclassified and written off as a credit loss. Credit card application fraud losses will increase from US$1.2 billion in 2016 to $2.1 billion in 2020 (Figure 10).[5]

5. See Aite Group's report *Application Fraud Rising as Breaches Fan the Flames*, March 2016.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 10: U.S. Application Fraud



Source: Aite Group

CNP FRAUD

Card-not-present transactions are just that—transactions in which the payment card is not present. While the contact center comprises a portion of these transactions, digital transactions originating from the online and mobile channels represent the lion's share of CNP volume. U.S. digital commerce is growing at a healthy clip, averaging 15% to 16% year-over-year growth for the past five years.[6] A testament to U.S. issuers' and merchants' investments in fraud prevention, CNP fraud actually plateaued at US$2.8 billion from 2013 to 2014, meaning that the good guys were actually gaining ground. The happy state soon passed, however, and CNP fraud resumed its steady growth in 2015, rising 14% from 2014 to 2015.

While nearly all FIs interviewed are seeing some degree of CNP fraud increase, the rate at which it is rising varies considerably. Some FIs report modest increases, while others are seeing a sharp uptick. One FI reports seeing a "linear increase," with its CNP fraud nearly doubling year over year. A few FIs are seeing brute-force attempts on the CVV2 increase; while some FIs limit this with rules and velocities, others do not, because according to their analysis, the CVV2 is "completely nonpredictive" of fraud.

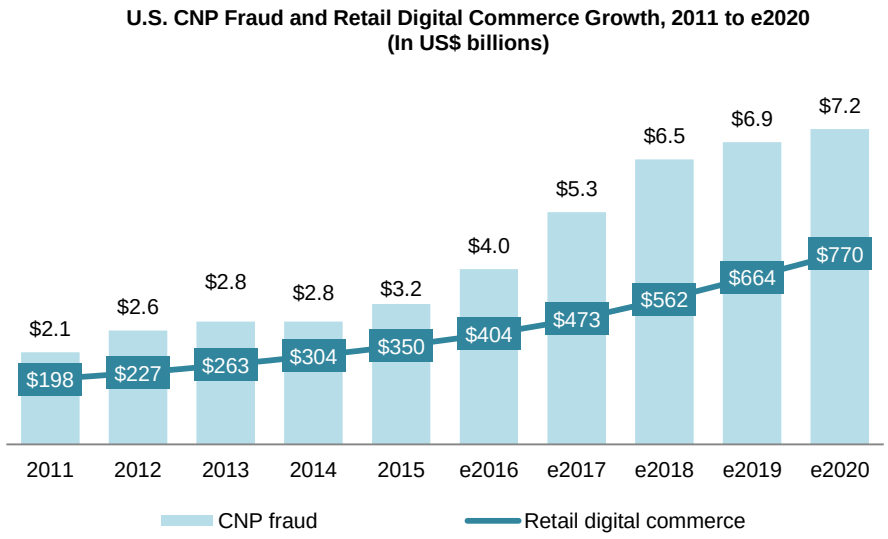
With only 20% of credit card transactions chip-on-chip, it's too soon to blame the rise of CNP fraud on the EMV migration. The more likely culprit is the vast quantity of compromised data at criminals' disposal. While a good portion of the fraud uses stolen card numbers, account takeover using compromised credentials is a leading cause of fraud for many CNP merchants.

6. See Aite Group's report *E-Commerce and CNP Transactions: Explosive Growth, Explosive Risk*, February 2015.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

As the U.S. migration to EMV progresses, the combination of continued strong growth in e-commerce, ready availability of consumer data and credentials on the underweb, and disappearing counterfeit fraud opportunity will create a perfect storm that will result in a sharp rise in CNP fraud (Figure 11).

Figure 11: U.S. CNP Fraud



Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

BEATING THE BAD GUYS

Amid all this doom and gloom, the good news is that issuers and merchants can use a number of technologies to help detect and mitigate the fraud. Table B lists some that can help with fraud prevention in the increasingly digital transaction environment. Fraudsters have proven capable of compromising any single point solution, so the best practice is to deploy multiple technologies in a layered manner. The first line of defense should consist of technology that operates behind the scenes and doesn't intrude on the user experience; the first five technologies in the table all offer this low-friction quotient. The remaining solutions in the table require customer interaction, so are more appropriately used as stepped-up authentication mechanisms as FIs work to balance security with a good user experience.

Table B: Digital Security Solutions

Technology	Description	Friction quotient
Device fingerprinting/ Digital identity assessment	Digital identity technology examines a combination of identifiable hardware and software attributes associated with a computer or mobile device. The resulting unique fingerprint can be used to provide recognition of devices associated with fraudulent activity as well as ongoing recognition of devices with trusted reputations. The mobile browser environment can be challenging to fingerprint, since there are fewer parameters to track than in the online browser environment. Mobile apps are just the opposite—digital identity vendors provide software development kits to dive deep into the device and create a footprint around parameters such as the number of contacts, number of songs in playlists, etc., as well as create behavioral analytics around the ways in which those parameters change. The device reputation providers that have deep consortiums are also valuable in proactive detection of repeat offenders. The ability to track personas created by combining multiple device fingerprints with other data elements such as email address are increasingly important to a number of executives interviewed for this report. It is also important for a device-fingerprinting solution to be able to detect the use of proxies. Cybercriminals use proxy servers to log on to bank websites from a proxy IP address that allows penetration of user accounts via the genuine end-user IP to gain positive device identification. Proxy attack detection can determine when a login or transaction is being performed via a proxy that is anomalous to the user by identifying the true IP used.	Low
Behavioral analytics	Behavioral analytics detect fraud by monitoring the user session to detect suspicious activities or patterns. These manifest in a couple ways: (1) Transactional anomalies**:** The user is performing transactions that are out-of-pattern compared with normal behavior. (2) Navigational anomalies**:** The manner in which the user is navigating the website is inconsistent with his or her own usual pattern, the pattern of his or her peer group, or is indicative of the navigational pattern of a bot.	Low

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Technology	Description	Friction quotient
Behavioral biometrics	Behavioral biometrics, also known as cognitive analytics, evaluate the manner in which a person is interacting with his or her device (PC, tablet, or smartphone) to determine whether it is consistent with the user's previous interactions, indicative of bot activity, or a fraudster.	Low
Malware detection	Once resident on a user's computer, this technology can be used to detect indicators of Trojan activity in a few ways: HTML injection detection: Detects and flags fraudulent changes to the end user's browser display via Man-in-the-Browser attacks, which attempt to either manipulate payments or harvest additional user credentials like a Social Security number, credit card number, or PIN. Man vs. Machine protection: Defends against advanced Trojans using automated script attacks to fraudulently add payees and transfer money to mule accounts. Man vs. Machine protection can determine whether mouse or keystroke movements are associated with user-directed actions. Server-side detection can detect code changes and other clues indicative of malware.	Low
Mobile operator data	A handful of vendors provide device authentication services in the North American market through direct, real-time interfaces with mobile operators. These vendors use the same device hardware-based network authentication as mobile operators use to secure their own services (e.g., SIM card) to provide positive verification that the device belongs to the person authorized on the mobile account as well as to provide notification if the device is lost or stolen.	Low
Knowledge-based authentication (KBA)	KBA questions seek to establish the authenticity of the end user by asking questions only that individual should know. KBA questions are either static (preset at the time of account setup) or dynamic (multiple-choice questions gleaned from databases including credit and/or demographic data).	High
Out-of-band authentication (OOBA)	In order to involve a second mode of communication, OOBA uses a communication mechanism that is not directly associated with the device being used to access the banking application. This is often accomplished by using a mobile device in conjunction with an online session to deliver a one-time password.	High
Transaction signing	Transaction signing requires the end user to digitally sign each transaction. The approach can vary: Some signing solutions use public key infrastructure on a hardware device, other solutions enable the end user's mobile device with the signing solution.	High
Biometrics	Technology that identifies people using physical characteristics or traits.	High

Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CONCLUSION

As the United States works its way into the ranks of chip-capable countries, issuers and merchants alike need to be prepared for significant shifts in the fraud landscape. Unfortunately, the bad guys aren't going to close up shop and find real jobs—they'll simply shift their focus to different attack vectors. Here are a few recommendations for players in the space.

For issuers:

- **If the bulk of your active cardholder population will not be upgraded by the end of 2016, find a way to accelerate your plans.** The data shows that criminals are already focusing their counterfeit card attacks on banks that have not yet upgraded to EMV. Meanwhile, banks that have been more proactive in their chip-card conversion are seeing rapidly declining net counterfeit fraud losses. This trend will only be exacerbated as the chip-on-chip transaction percentages increase and criminals focus their counterfeit attacks on unprotected bank identification numbers (BINs).
- **Invest in solutions that can help to mitigate the rising tide of account takeover, application fraud, and CNP fraud.** All of these forms of fraud are already on the rise, thanks to the vast amount of data at criminals' disposal. The gradual whittling away of US$4 billion in counterfeit card fraud creates further incentive for criminals to transition their attacks to other methods. FIs need to invest in layers of technology that can help detect this fraud while preserving the user experience.
- **Watch out for the ATM.** This is another attack vector that has been a big pain point in Europe and is a rising concern in the United States. Upgrade your ATM to support EMV and invest in technologies to prevent lower-tech schemes such as cash-trapping.
- **Continue working on consumer education.** People are creatures of habit, and the process of changing their behaviors is rarely painless. With two different card-verification methods in the U.S. market, the confusion is heightened, particularly on the debit side, where the shopping experience can vary widely depending on each merchant's configuration.

For merchants:

- **Bolster your CNP fraud controls.** CNP fraud is already on the rise, and the problem will get worse before it gets better. Merchants must invest in layers of technologies that will help detect fraud while maintaining a delightful user experience.
- **Prioritize reterminalization.** If you haven't reterminalized yet, chances are that the pain associated with this is already manifesting in your monthly statement from your acquirer. With certification queues still lengthy at acquirers, merchants that haven't started planning their EMV migration need to be prepared for a significant uptick in counterfeit fraud chargebacks.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

Application Fraud Rising as Breaches Fan the Flames, March 2016.

Not Your Father's 3-D Secure: Addressing the Rising Tide of CNP Fraud, February 2016.

Combating Fraud: Consumer Preferences, January 2016.

Digital-Channel Fraud Mitigation: The Mobile Force Awakens, June 2015.

E-Commerce and CNP Transactions: Explosive Growth, Explosive Risk, February 2015.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is an independent research and advisory firm focused on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, securities & investments, and insurance, Aite Group's analysts deliver comprehensive, actionable advice to key market participants in financial services. Headquartered in Boston with a presence in Chicago, New York, San Francisco, London, and Milan, Aite Group works with its clients as a partner, advisor, and catalyst, challenging their basic assumptions and ensuring they remain at the forefront of industry trends.

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

101 Arch Street, Suite 501, Boston, MA 02110 • Tel: +1.617.338.6050 • Fax: +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com