White Paper

LexisNexis® Card Issuer Fraud Study

Issuers Confront Application Fraud and Account Takeover in a Post-EMV U.S.

June 2016

LexisNexis® RISK SOLUTIONS | Financial Services

Table of Contents

Table of Figures

Introduction

Card fraud is a multibillion-dollar moving target that continues to become ever more complicated for issuers due to the introduction of new channels and products. In fact, over the last year the rate of fraudulent new account openings increased 113%, according to Javelin's 2016 Identity Fraud report.[1] Confronted with the implications of the U.S. EMV rollout, mobile wallets, and digital channel applications, issuers are faced with significant headwinds as they attempt to stay a step ahead of fraudsters. This study examines the effects that the aforementioned challenges will have on the ability of issuers of credit, debit, and prepaid cards to mitigate card fraud, with a specific focus on how issuers can most effectively manage application fraud and account takeovers in this dynamic environment.

Executive Summary

Key findings

Issuers directly lose $10.9 billion to card fraud each year: These losses are driven principally by credit cards, which accounted for 71% ($7.6 billion) of the losses while debit accounted for 25% ($2.7 billion). Driven by a lower relative number of cards in the market, prepaid cards contributed to only $0.5 billion in fraud losses.

Credit cards result in three times the fraud loss per card compared with debit: With a comparable number of credit cards and debit cards in circulation, this difference in overall losses translates to significantly greater losses per card for credit compared with debit ($9 vs. $2.80 per card, respectively). Prepaid cards, much fewer in number than credit and debit, slot in between at $4.70 per card.

Issuers' opinions are mixed about some aspects of the effect that EMV will have on fraud: The majority of issuers agree that EMV will result in increased card-not-present (CNP) fraud losses, while driving a reduction in fraud at the point of sale (POS). Despite the EMV rollout, counterfeit card fraud is the fraud type issuers believe is most likely to increase as criminals rush to misuse magnetic-stripe cards before that opportunity ends.

Late adopters of EMV are rightfully more concerned about application fraud: The level of concern about application fraud among issuers that are late adopters of EMV is double that of the early adopters. Nonetheless, while early adopters of EMV are less concerned, their experiences certainly prove the late adopters' fear is well-founded. Twenty-two percent of the losses experienced by issuers in the top 50% of EMV-capable issuers by portfolio share could be traced to application fraud, compared with 17% of the losses among those in the bottom 50%.

Detecting synthetic identities is even more troublesome for financial institutions than stolen identities. Misused true identities that slip past bank security measures may eventually be detected by the victims through review of their credit report. Because synthetic identities are constructed from identifiers that are not clearly associated with an individual with established credit, there is no one to detect the fraud besides the targeted FI. Nearly a third of application fraud is created from identities that have never before been seen by a FI, making it nearly impossible to validate the PII through conventional means.

Using more fraud prevention solutions does not necessarily equate to less application fraud: Issuers with higher than average rates of application fraud are generally more likely to use any fraud prevention solution or control. This point suggests that issuers are applying as many tools as possible, but they're having little success because they aren't doing so strategically.

Manual reviews afford most issuers the 'gut check' they need to control for fraud: The value that manual reviews provide is apparent in their prevalence among issuers: 63% have separate manual review processes for both credit underwriting and fraud, while 33% at the least integrate the review for both into a single process.

Coordinating with affiliates complicates fraud mitigation: For both application fraud and account takeovers, issuers specified that detecting fraud was most difficult when it came through one of their affiliates' channels, such as a co-brand or private label partner – either in person or online. This indicates the difficulty of coordinating a fraud mitigation strategy across multiple organizations where incentives may be at odds.

Issuers believe takeovers are under control, but they worry about customer experience and growth related to mobile wallets: Mobile wallets are seen as a unique area of concern around the growth of account takeovers, and many issuers (56%) believe that they cannot further reduce takeovers without hurting the customer experience.

Customer service-oriented call centers are serious contributors to the problem of account takeovers: To accomplish account takeover, fraudsters will frequently target customer service representatives as the weakest link in the account access process. Recognizing this problem, 41% of issuers indicate that successful social engineering of customer service staff is either the most or second most difficult challenge in mitigating account takeover.

Significant investment in fraud mitigation is planned for 2016: A strong majority (78%) of issuers are planning to make significant investments in fraud mitigation over the next 12 months, with most planning to invest in additional tools. Dynamic and static KBA (knowledge-based authentication) lead the list of tools targeted for additional investment, followed by mobile carrier identity verification and manual reviews.

Recommendations

Prepare for the impact of EMV by bolstering application fraud and account takeover prevention capabilities: Investment in fraud mitigation solutions and strategies designed to more effectively prevent application fraud and account takeovers, especially on more valuable credit card accounts, should be made immediately as the U.S. EMV rollout is well under way.

Look beyond applicant-provided data: In light of the vast array of data breaches over the past few years, supplementing applicant-provided data with additional dynamic data sources (e.g. device fingerprinting/reputation) is key in addressing both application fraud and account takeover.

Implement the use of an identity scoring platform to maximize ROI on fraud mitigation solutions: These platforms help determine when automated solutions or strategies are being implemented effectively or require adjustment so that issuers can be assured that they are achieving the best return on their fraud mitigation investments.

Open regular lines of communication with affiliates about fraud threats that have shared implications: The relationship between issuers and affiliates can be complicated by differing incentives. To move beyond individual motivations and to secure buy-in for changes needed in fraud mitigation strategies or solutions, both parties can benefit from an understanding of how threats could result in shared losses of customers and revenue.

Continue to improve accountholder and device verification during mobile wallet enrollment or provisioning: By leveraging solutions that are more difficult to circumvent, such as biometrics, issuers can be assured that the individual enrolling or provisioning a card to a mobile wallet is legitimate.

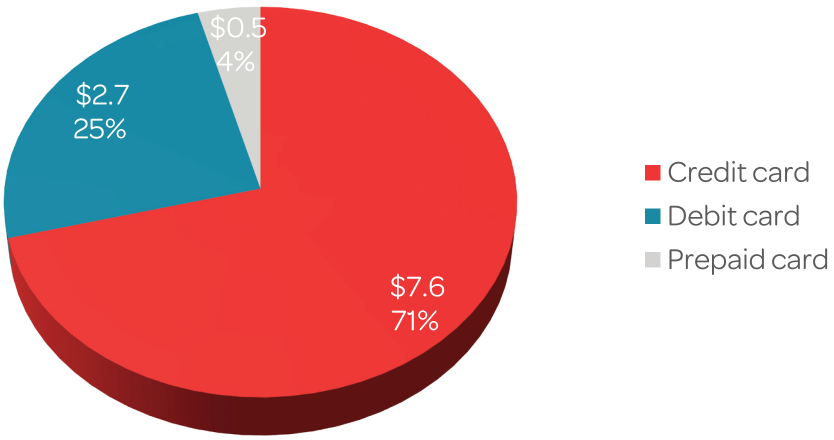
Move beyond the verification of PII at the call center to prevent account takeovers facilitated through the channel: Voice biometrics can more effectively identify legitimate cardholders, especially if there are previous call center interactions, which can be used to establish a voice print. Even when the legitimate cardholder has not previously called the institution, voice biometrics can screen the caller to determine if this individual has previously been associated with fraud.

Overview

General trends

Ever since the first credit cards were introduced over 60 years ago, convenient "plastic" has been on an inevitable path to ubiquity.[2] Today, transactions using payment cards – including credit, debit, and prepaid – represent nearly three-quarters of the dollars spent at the point of sale (POS) and an even greater proportion of online spending.[3,4] But wherever money changes hands, fraud is not long to follow. The diverse, perennial challenge of card fraud contributed to $10.9 billion in losses for issuers over the past year (see Figure 1). Worse still, the very nature of fraud is to obfuscate the truth, meaning that success in identifying it is anything but clear.

Issuers Suffered $10.9 Billion in Card Fraud Losses

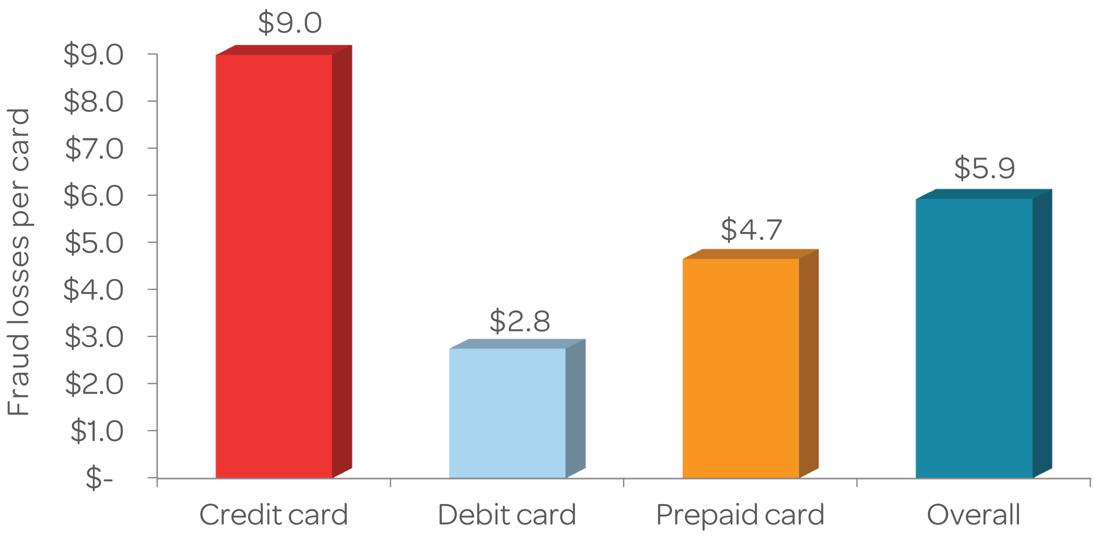


* Weighted data

Figure 1.Total Card Fraud Losses Experienced by Issuers in the Past 12 Months

Among the three major card types, credit cards are favored most by fraudsters. With credit cards representing 71% of all card fraud losses for issuers in the past year, credit limits make more attractive and valuable targets for fraudsters than available funds in a depository account (see Figure 1). With a comparable number of credit cards and debit cards in circulation, the difference in overall losses translates to significantly greater losses for credit cards over debit cards ($9 vs. $2.80 per card, respectively). Prepaid cards, which are much fewer in number than credit and debit, were associated with $500 million in fraud losses, or $4.70 per card (see Figure 2).

Compared With Debit Cards, Credit Cards Drive Over Three Times the Losses per Card



* Weighted data

Figure 2.Fraud Losses per Card in Portfolio, by Card Type

No single scheme or constituent party is responsible for facilitating the majority of card fraud. Two of the most pernicious types of card fraud, application fraud and account takeover, each represent 20% of total fraud losses. Fueled by data breaches, but on its way to being eradicated (see EMV and Issuer Expectations for Fraud section, pg. 10), counterfeit cards are responsible for 16% of total losses (see Figure 3).

> "We have a hard time discerning between first party fraud, third party fraud, and credit risk. When you can't confirm identity theft, it falls into the collection bucket. Can't say we have a good grasp on it, but it doesn't get enough attention."
>
> Fraud Executive, Regional FI and Credit Card Issuer

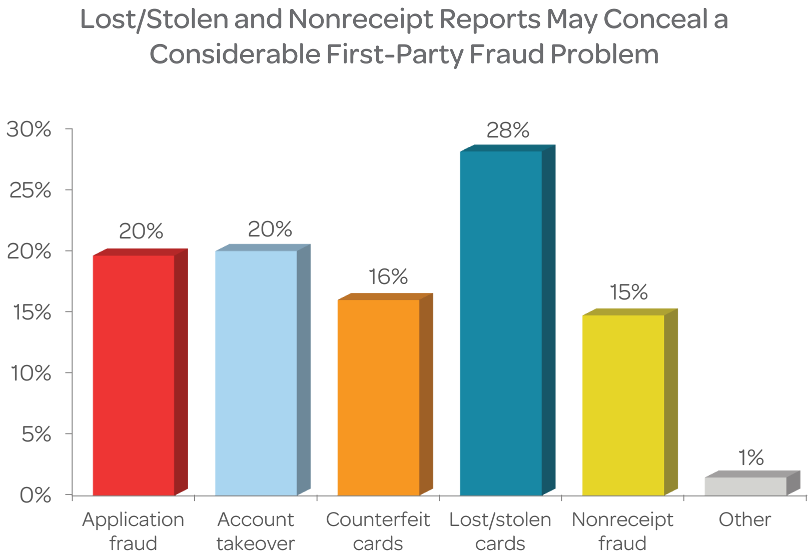


Figure 3.Proportion of Total Card Fraud Losses, by Type of Fraud Scheme

The misuse of payment cards that are lost or stolen (28% of total fraud losses) and nonreceipt fraud (15% of total fraud losses) represent the two schemes most likely to confound issuers' ability to discern between fraud committed by the cardholder and a fraudster (see Figure 3). Under pressure to identify if fraud has occurred, manage risks associated with a variety of fraud schemes, and determine who is responsible, issuers clearly have their work cut out.

EMV and issuer expectations for fraud

The impact of EMV on fraud has been a heavily anticipated event among U.S. payment industry stakeholders for the past few years, for both positive and negative reasons. Whenever successful fraud mitigation technology and processes are introduced, they effectively exert pressure on fraudsters to find other people, places, or products to target. Issuers share many of the same expectations about how fraud will shift as EMV is rolled out in the U.S., though their progress in the actual EMV-issuance process directly influences these expectations.

EMV cards contain a tamper-resistant chip that represents the key to its ability to control for fraud. Beyond being nearly impossible for criminals to replicate, these cards also generate cryptograms that are sent alongside the traditional primary account number (PAN) and expiry date for use in the authorization process. The cryptograms are unique to each transaction, largely eliminating any incentive to compromise, or opportunity associated with compromising, the payment credential. Considering these two fraud-mitigating characteristics of EMV cards, it is no surprise that 76% of issuers believe that EMV will reduce losses from fraud at the POS for their institutions (see Figure 4). This has been experienced in other markets, including the U.K. and Canada, and is rightly anticipated by U.S. issuers.

Issuers Anticipate EMV's Benefits for POS Fraud and Fear Negative Consequences for CNP Fraud

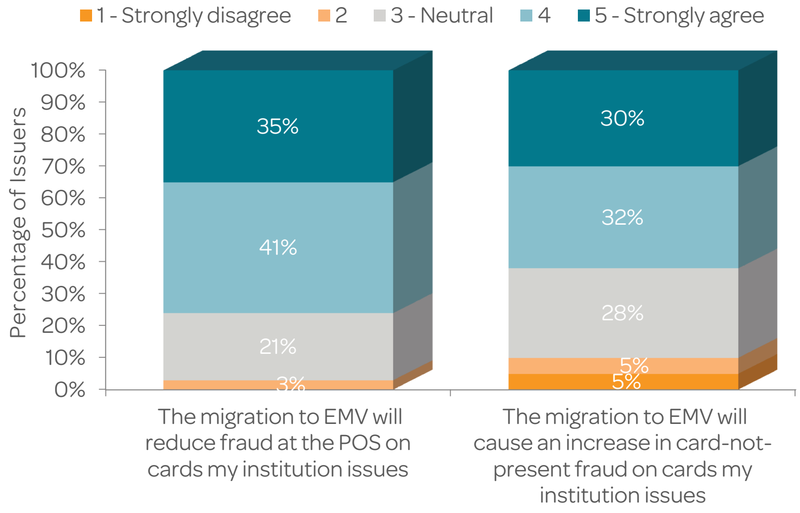


Figure 4.Issuers' Attitudes Toward How EMV Will Affect Fraud in the U.S.

> "EMV will have a good impact on counterfeit, but given the inherent capabilities of mobile devices, with an ecosystem that leverages them, we will get stronger overall from a secured card perspective."
>
> Fraud Executive, Large National FI and Credit Card Issuer

As EMV cards and terminals become more common, many stakeholders anticipate fraudsters will turn their efforts toward counterfeiting payment cards and the CNP channels. This expectation is not surprising as CNP fraud also involves the use of payment cards and targets merchants, but the 62% of issuers anticipating growth in CNP fraud due to EMV may be only partly correct (see Figure 4). Rather than throwing up their hands after the EMV rollout and participating in a wholesale shift from card fraud at the POS to CNP channels, fraudsters in other markets looked for other ways to maintain their destructive business.

Card Counterfeiting Expected to Grow Regardless of EMV Issuance Progress

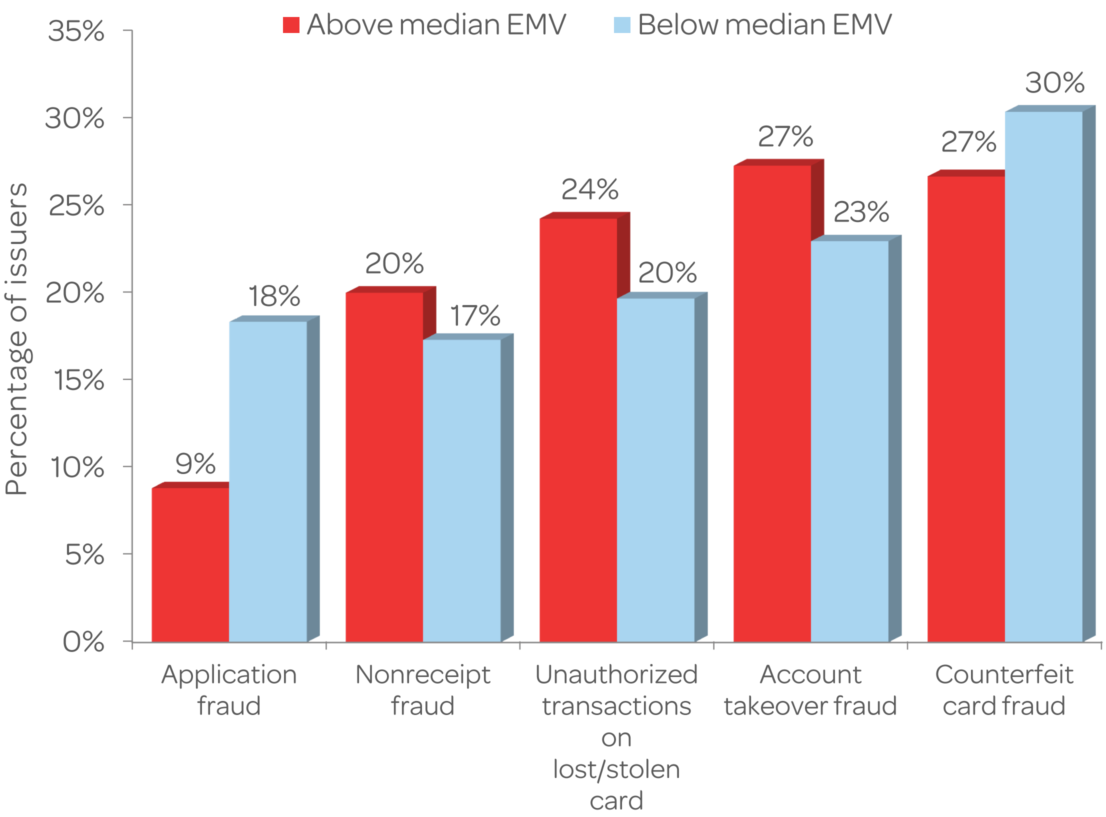


Figure 5.Issuers Expecting Fraud Types to Increase Over Next 12 Months, by EMV Issuance Status

Success in committing fraud, like many other things, is a matter of planning and practice. Fraudsters that have found success in POS card fraud are unlikely to immediately give up what may represent an enterprise with years invested in its success. Rather than shifting immediately to CNP, fraudsters in the U.K. turned to application fraud and account takeovers at the POS. As such, U.S. issuers would be right to expect application fraud and ATO to increase in the next 12 months. CNP fraud, on the other hand, is a significant problem in the U.S. that was expected to increase with or without EMV.[5]

The industry's domestic and international experiences associated with EMV issuance and the perceptions of application fraud risks are fairly intertwined. Concern over application fraud among the bottom 50% of issuers in terms of cards in their portfolio which are EMV-capable is double that of the top 50% (18% vs. 9%, respectively). While early adopters of EMV are less concerned, their experiences certainly prove the late adopters' fear is well-founded. Twenty-two percent of the losses experienced by issuers in the top 50% by EMV capability could be traced to application fraud, compared with 17% of the losses among issuers in the bottom 50% (see Figure 6).

> "We expect that as EMV adoption ramps up (in the US) it will put pressure on the ID theft space, specifically application fraud and account takeovers."
>
> Fraud Executive,
> Large International FI and
> Credit Card Issuer

EMV-Heavy Issuers Are Experiencing More Application Fraud Than Lagging Peers

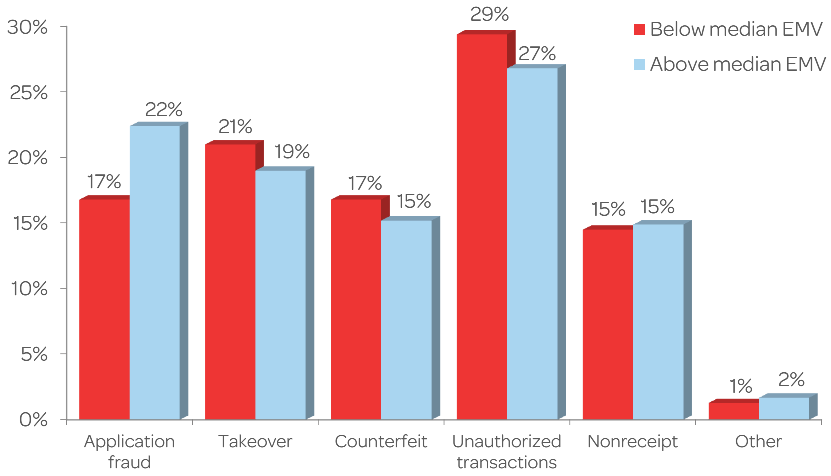


Figure 6.Proportion of Fraud Losses by Type, by EMV Issuance Status

Also quite telling is where EMV haves and have-nots agree, specifically that counterfeit fraud is the most likely to increase in the next 12 months (see Figure 5). With full adoption of EMV still a few years away,[6] fraudsters may take advantage of the closing window for card counterfeiting. Despite this concern, issuers may still have yet to reissue a large portion of their portfolio, indicating that other considerable roadblocks are holding them back. Ultimately these and other concerns around mobile wallets (see ATO Evolves with the Market section, pg. 23) will motivate 3 in 4 issuers to make significant investments in fraud mitigation in the coming year (see Figure 7).

Among Issuers Planning Investments, Fraud Mitigation Tools Top the List

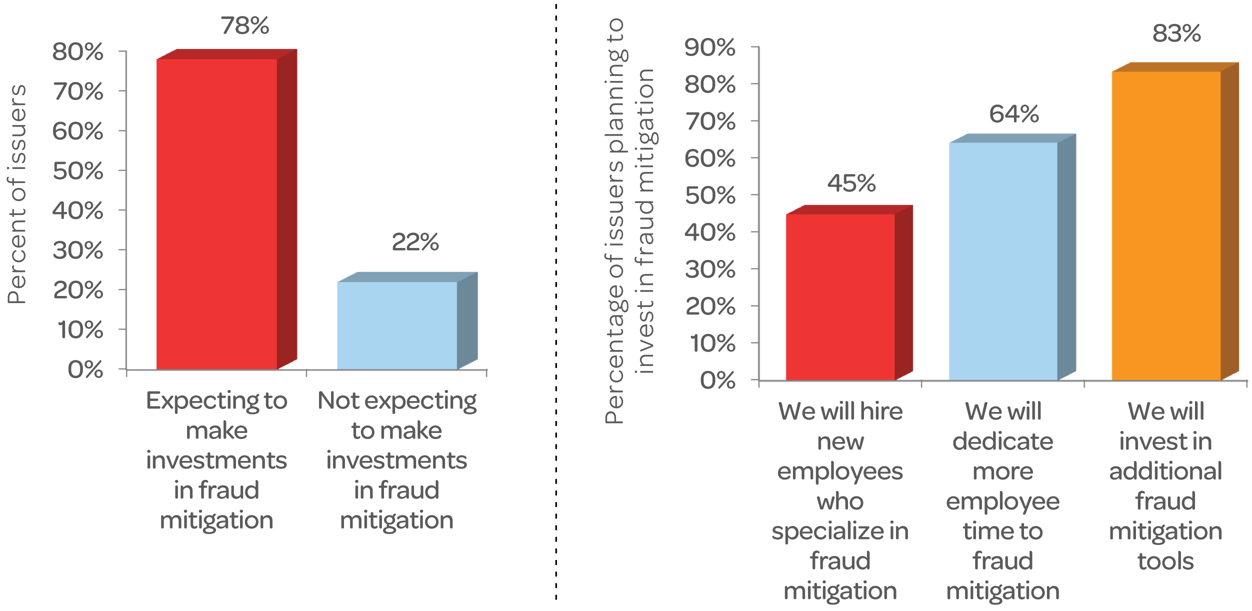


Figure 7.Issuers Planning to Invest in Fraud Mitigation and Their Planned Areas of Investment

Application Fraud

Stolen vs. synthetic identities

Fueled by data breaches, fraudsters have access to a vast array of PII, many of which will remain useful for the entire life of the victim. In 2014 alone, 61.8 million individuals indicated that they had been notified of a data breach. Of these individuals, 4.3 million had their Social Security number compromised.[7] With this much available data, it is no surprise that stolen identities drive the majority of new account fraud. Forty-one percent of fraudulent applications are composed entirely of stolen identifiers (i.e., true identities) and 27% are only partially composed of stolen identifiers (i.e., manipulated identities), (see Figure 8).

True Identities Are Prevalent in Application Fraud, but Synthetic Identities Follow Closely

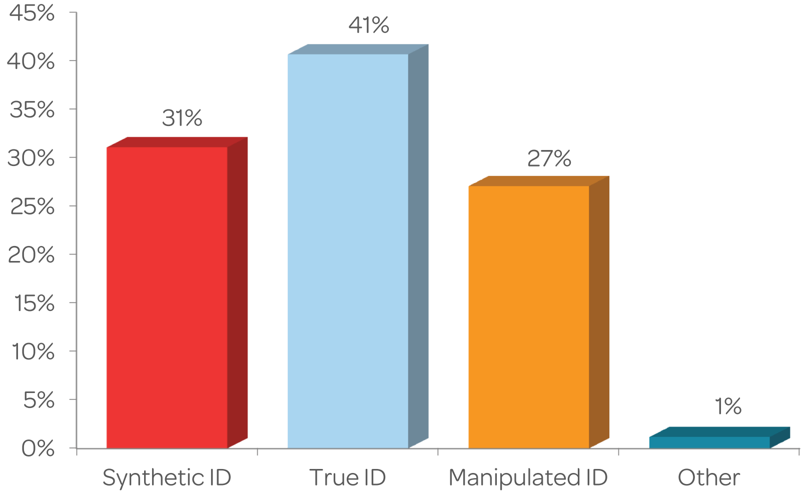


Figure 8.Application Fraud Types, Percentage of Attempted Fraudulent Applications

Detecting synthetic identities is even more troublesome for financial institutions than stolen identities. Misused true identities that slip past bank security measures may eventually be detected by the victims through review of their credit report. Because synthetic identities are constructed from identifiers that are not clearly associated with an individual with established credit, there is no one to detect the fraud besides the targeted FI. Nearly a third of application fraud is created from identities that have never before been seen by a FI, making it nearly impossible to validate the PII through conventional means.

"The ongoing data compromise events are continuing to present a challenge. We will need to rely on higher levels of authentication than we have before. The whole authentication space is really tough because of the limited elements we have – they are all static and easy to compromise from a number of sources such as phishing, breaches, etc."

Fraud Executive,
Large International FI and
Credit Card Issuer

Moreover, since these identities appear simply as thin-file applicants, there are minimal fraud red flags that can be associated with the initial application. During a successful fraud attempt, if the targeted FI is simply validating PII provided during the application it will see data points that are unlikely to be connected to any other individual. Consequently, there is no mismatch of information nor are there multiple claims to unique identifiers such as Social Security number.

While the identifiers used in synthetic identity applications are not clearly associated with any individual with established credit, this does not mean that no consumers are victimized by this type of fraud. The identities of minors with no current financial accounts and no credit file offer a blank slate for criminals to construct their own identity. This leaves victims with a blemished credit history before they even own any accounts and forces them to slash through years of fraud to regain ownership of their identity.

While approved thin-file applications typically have restrictions on available credit, due to their lack of history, they still offer fraudsters a foot in the door. With an approved account, the criminal can cultivate this account, masquerading as an ideal accountholder making regular purchases and payments to build credit, eventually raising the credit limit and maximizing their payoff before abandoning the account in a scheme known as a "bust out." Alternatively, they can use the initial account as a platform to acquire additional banking products.

Managing fraud via affiliates

Affiliate relationships can be important drivers of new business for an issuer, especially when they represent co-branded or private-label cards. Issuers should be cautious, however, as affiliates' websites is the channel where issuers reported having the most difficulty in detecting fraudulent applications (see Figure 9). In person at affiliates' locations was ranked third. Managing these difficulties is anything but easy as a number of factors complicate the fraud mitigation process for cards issued through affiliates.

Applications From Affiliates' Websites Are the Most Difficult to Screen for Fraud

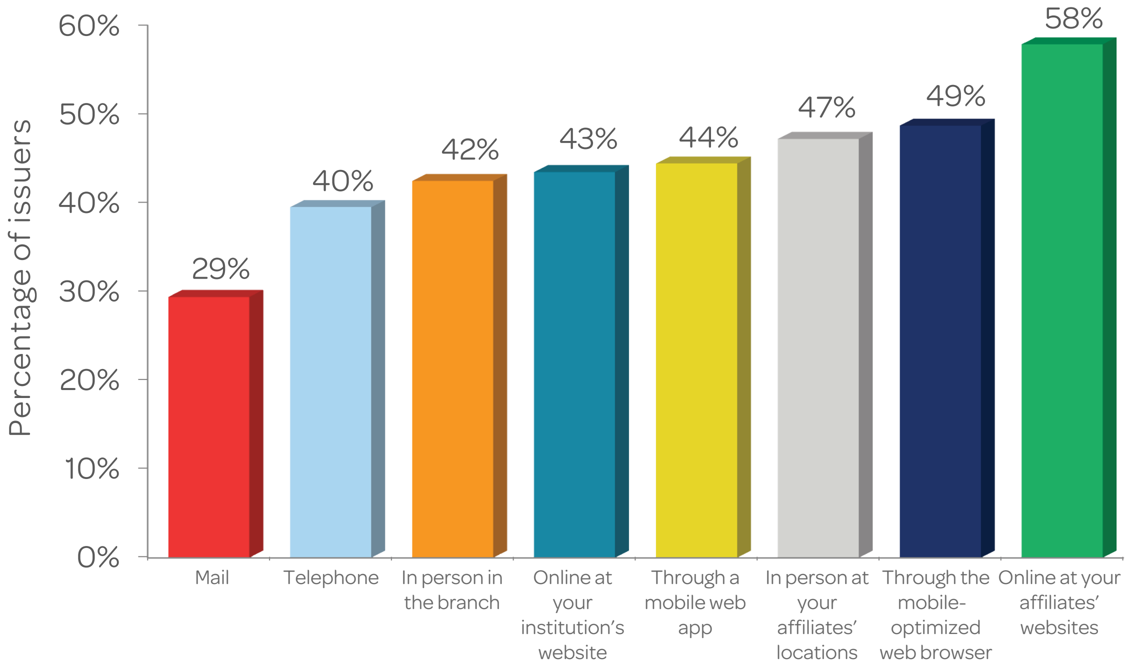


Figure 9.Difficulty of Detecting Application Fraud by Channel

First, the issuing institution has limited control over many parts of the application process, especially for in-person applications. To the extent that applications are submitted through the partner's systems and not routed directly to the issuer, legacy hardware and software may limit the digital channel-specific fraud mitigation solutions, reducing the issuer's visibility into the card application beyond what is transmitted secondhand. Even if in-person applications are routed to a site controlled by the issuer, they remain out of the issuer's control in many ways.

Since these applications are processed by the affiliate's staff, the issuer has limited control in training the staff. This training is key, because many of these individuals will likely handle new card applications as only an ancillary part of their responsibilities. Without regular exposure to new account opening, they are less likely to notice discrepancies in identity documentation that may indicate fraud.

Moreover, in a physical store, the stakes are higher for the affiliate in turning down a legitimate application. A customer applying for a new card in-store is likely to have a shopping cart full of items they intend to purchase. Declining the application suggests an immediate loss of revenue. Additionally, unlike for an online application, in-person applications are likely to be conducted in the presence of other shoppers, which means that a negative experience by one potential customer can effect a negative experience for the other shoppers.

Voice of the executive: The challenge of conflicting incentives

A particular challenge called out by industry executives is how the incentive mismatch for managing fraud can complicate the process — when one entity receives the gain from signing new card applications while another bears the risk from fraudulent applications. In affiliate/co-branded relationships, this is likely to be the case, since new store-branded cards are likely to be tied to additional revenue for the issuer's partner, but charge-backs resulting from in-person fraud may be placed with the card issuer or at the least adversely affect the longevity of the relationship.

An example of conflicting incentives is when issuers are compelled by their affiliate to provide instant credit after approval. The need to convert applicants into instant in-store or online revenue bypasses the time-consuming but effective manual reviews and could actually contribute to a higher rate of fraud.

> "The most significant challenge would probably be an increasing desire by the business to offer instant approval via the web. Apply online, get instant ability to purchase. It is problematic because it defeats a pretty key control of being able to mail a card to an address. When you give up mailing of the plastic, it opens the door for someone to apply with true victim info. They experience this in a private label business."
>
> Fraud Executive,
> Large International FI and
> Credit Card Issuer

Identity verification vs. Fraud mitigation

Vetting of information provided during the application process is motivated by two separate and sometimes complementary goals: identity verification and fraud mitigation. During identity verification, which is closely tied to regulatory compliance, the issuer attempts to confirm that the PII provided can be traced to a known individual. Yet even if the data point is valid it does not confirm that the individual who provided it is the true owner of that PII, which is where fraud mitigation comes into play.

For both identity verification and application fraud mitigation, some form of knowledge-based authentication (KBA) led the list of solutions used during the application process. While dynamic and static KBA have received some criticism, most FIs, including smaller banks and credit unions, continue to find KBA to be an effective tool in preventing fraud. Only 5% of FIS report they use dynamic KBA solely for fraud mitigation; however, FIs report that dynamic KBA is their most used tool for identity verification (37%) or for both identity verification and fraud mitigation (34%). Conversely Static KBA is ranked highest solely for fraud mitigation (29%), but the lowest for identity verification (12%).

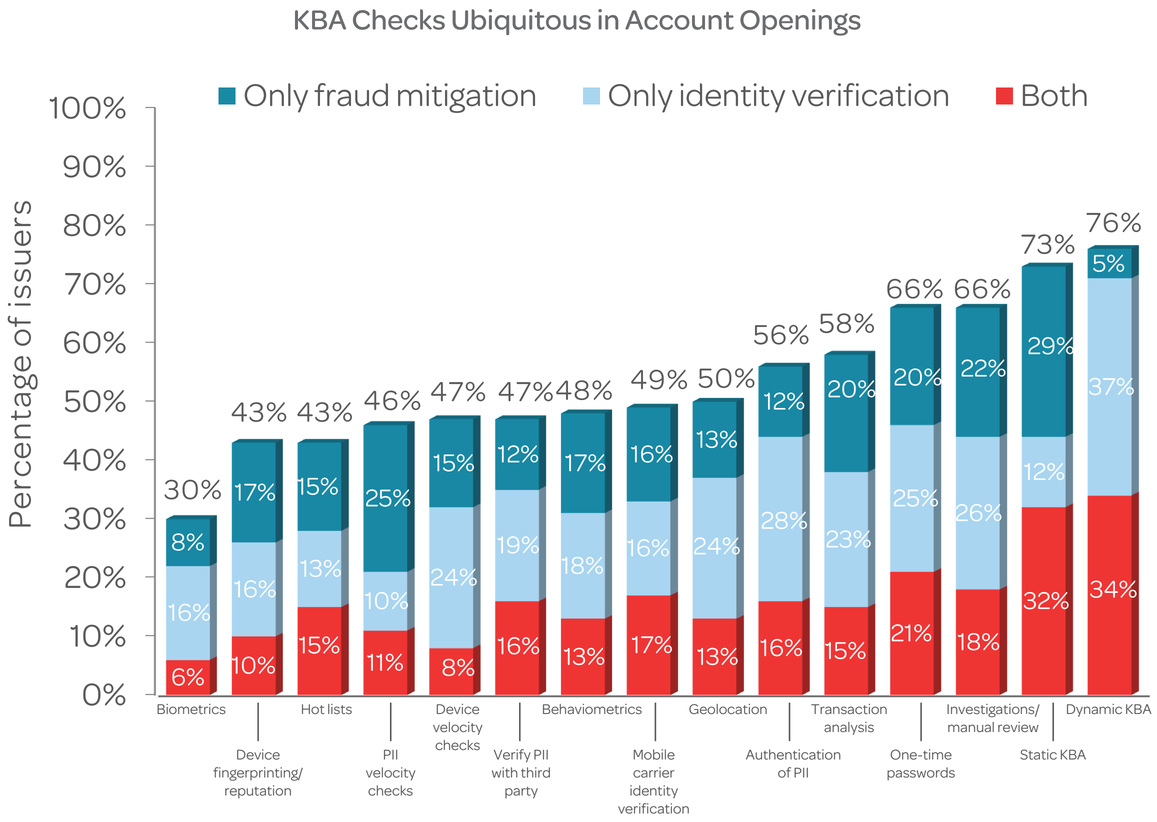


Figure 10.Use of Fraud Mitigation Solutions During Account Opening

As part of the U.S. Patriot Act, Customer Identification Program requirements hinge on the validation of a comparatively restrictive set of data points about the applicant. If an applicant provides obviously incorrect information, in most cases the application will be quickly terminated with little concern about alienating a legitimate customer. PII validation can function as the first barricade against fraud, but in isolation it is easily circumvented, because it relies on information that is comparatively easy to obtain on the black market. To FIs that rely solely on validating PII, as long as the information provided is consistent with the sources they use to validate it, there will be no distinction between the application of a legitimate or fraudulent individual.

The influence of fraud rates on the use of digital controls

Emerging fraud detection tools combat application fraud by gathering contextual data that is supplied involuntarily by the applicant. The less control individuals have over how information is collected on their application, the less opportunity they have to falsify that information. Solutions such as device identification/reputation, geolocation, one-time passwords, behaviometrics , and mobile carrier identification. Yet despite the promise of these solutions to tackle challenges distinct to the digital channel, issuers' experiences with differing rates of application fraud are having an impact on adoption and implementation that could undermine their effectiveness.

Based on the rate of use of different fraud prevention solutions among issuers with higher vs. lower than average application fraud, there are two clear themes. Firstly, some solutions are commonplace regardless of their effect on application fraud, being used in relatively equal proportions by issuers with both higher- and lower-than-average rates of application fraud. Second, issuers with higher-than-average rates of application fraud are generally more likely to use any solution. This second point suggests that issuers are applying as many tools as possible, but they're having little success because they aren't doing so strategically (see Leveraging Identity Scoring section, pg. 21).

Higher Fraud Issuers Are Using More Tools to Manage Application Fraud, but Is It Enough?

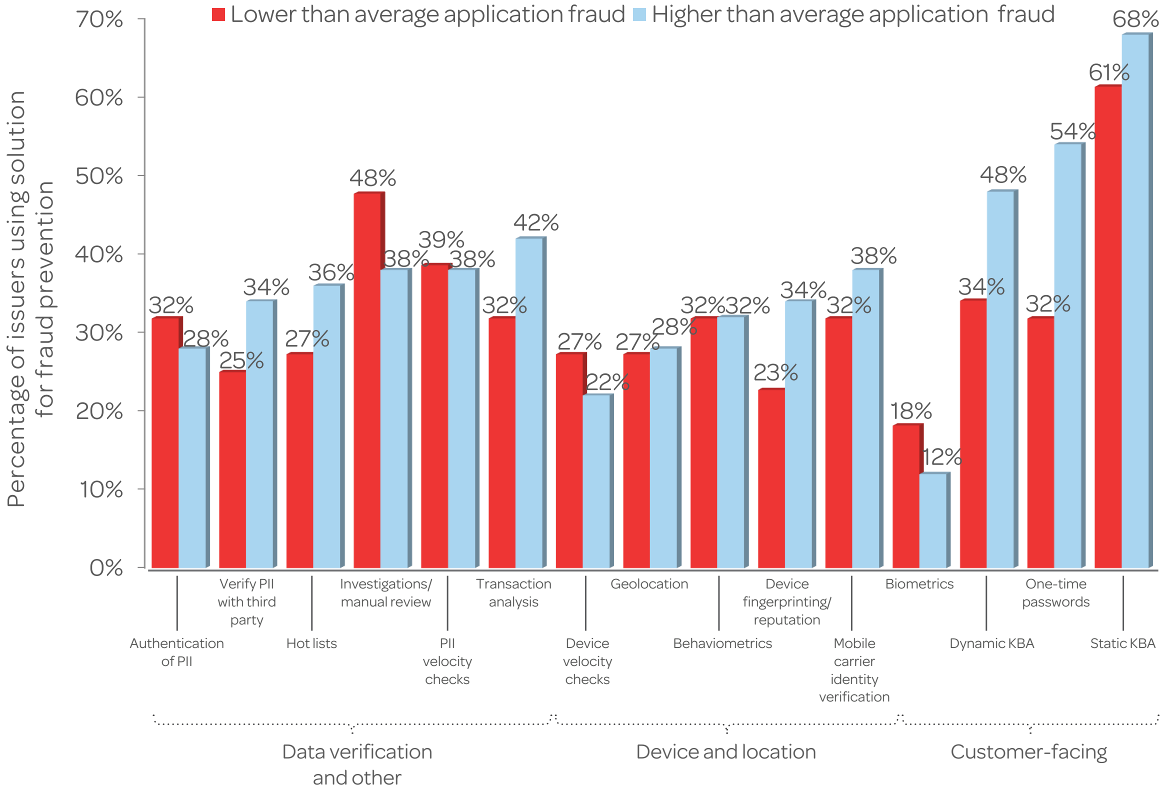


Figure 11.Use of Tools for Preventing Fraud During Account Opening, by Rate of Application Fraud

Device fingerprinting/reputation has the capacity to determine if the applicant is applying through a digital channel from a device with a known positive or negative reputation. A digital channel solution with a long history and which has continued to evolve in the challenging mobile environment, device fingerprinting/reputation still is used by only 34% of issuers with higher-than-average application fraud and only 23% of issuers with lower-than-average application fraud (see Figure 11).

IP address-based geolocation is the weakest of these five controls, since fraudsters have long had the capability to obfuscate IP addresses. However, the location of an applicant's mobile device can provide issuers significantly greater assurance that the applicant is in a location that can be reasonably associated with where he or she purports to be.

Issuers can use one-time passwords to ascertain (by cross-referencing other PII) whether the phone number provided during the application process is in fact in the possession of the applicant. Once largely the purview of industries such as financial services, these types of solutions are now commonly found in more digital, consumer-oriented services such as Facebook and Gmail. This is one of the tools with the greatest discrepancy in use between issuers with higher-than-average application fraud (54%) and lower-than-average application fraud (32%), (see Figure 11). Part of this discrepancy could be driven by an increased need among more fraud-challenged issuers, or a potential failure to implement these solutions effectively.

Issuers are also beginning to use emerging tools such as behaviometrics that measure how users interact with the digital application environment through their device, which can be a laptop, tablet, or smartphone. In instances where a device has been compromised and other solutions such as geolocation or device fingerprinting would not discern an issue, behaviometrics can be effective. Additionally, issuers are starting to look to mobile carrier identity verification that leverages billing and device data directly from the mobile carrriers.

Voice of the executive: Effectively leveraging controls with identity scoring

Considering the unique strengths and weaknesses of each solution, issuers should layer those that are most appropriate to the channel. Doing so provides the greatest overall coverage against the widest variety of threats. That said, even among solutions of the same type, not all are created equal and when they should be used is not always clear. Issuer executives recognized the need to reliably measure the impact of the solutions they implement and the circumstances under which they are used.

To that end, identity scoring platforms are recognized by executives for providing multiple benefits, the most important of which is ensuring that issuers are instituting the most effective approach to detecting fraudulent applications. This is achieved by analyzing available channel-specific and channel-agnostic solutions that enable the most complete view of the applicant. In instances where fraud persists despite the implementation of strategy to combat fraud, issuers can identify areas of weakness that may require supplemental solutions.

These platforms further add value by capturing and analyzing combinations of risk indicators that may not be useful on their own and which could be missed during a manual review (see Value of the Human Touch section, pg. 22). When used to help determine if automated solutions or strategies are being implemented effectively or require an adjustment, along with indicating when an individual application could benefit from a closer inspection, issuers can be assured that they are achieving the best ROI for their fraud mitigation investments.

> “If there was one thing to do it would be to focus on your process. Is that data that you have helping you understand how your controls are performing? Leverage that to make decisions going forward. The biggest challenge I am seeing at organizations is putting in a control without putting in some way to monitor for that control.”
>
> Fraud Executive,
> Large National FI and
> Credit Card Issuer

Value of the human touch: Manual reviews

Manual reviews are indispensable to FIs in managing fraud. No matter how robust an issuer's fraud detection system is, there will always be applications that fall into a gray area where they appear too risky to be automatically approved, but the case for fraud is not strong enough to justify an outright decline. These gray-area cases arise from situations that are both legitimate (e.g., a recent move places an applicant in a different geography than is on file) and illegitimate (e.g., a fraudster successfully confounds some of the issuers' security systems).

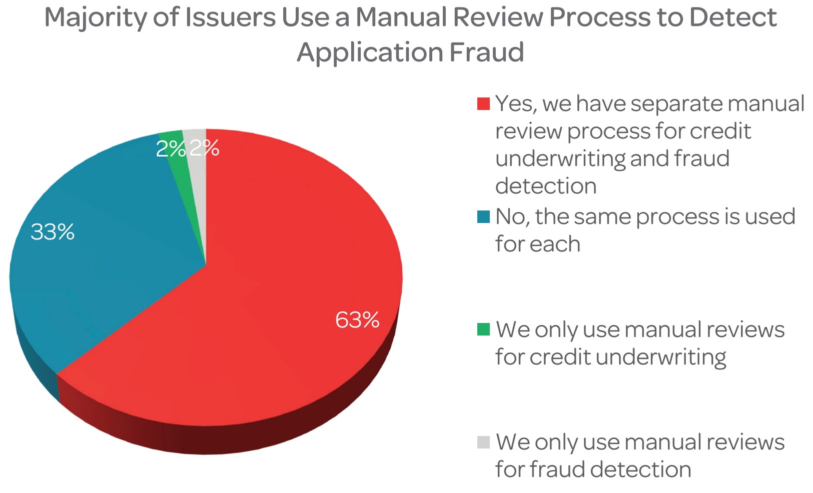


Figure 12.Manual Review Processes Among Issuers

For these gray-area applications, a human analyst can provide intuitive analysis of risk factors that automated systems don't necessarily detect. The value that manual reviews provide drives their prevalence among issuers: 63% have separate processes for both credit underwriting and fraud, while 33% at the least integrate the review for both into a single process (see Figure 12). However, manual reviews are not without their shortcomings. Human analysts are prone to error in processing application details and may overlook risk factors that are innocuous in isolation but indicate an elevated risk of fraud when combined with other factors.

What is more problematic is that manual review teams are comparatively expensive and difficult to scale on short notice if the volume of applications increases suddenly. This can generate backlogs during seasonal fluctuations in fraud, potentially weakening safeguards as processing capacity is strained.

Rather than existing in isolation, automated scoring systems can significantly boost the efficiency of manual review teams. By providing an overall risk score for each applicant and indicating the components that flag an application as either legitimate or fraudulent, these systems can help focus analysts' efforts on validating the parts of the application that require the most scrutiny (see Identity Scoring section, pg. 12).

"We coach and train our underwriters to stay out of robot mode. Take a holistic approach and use your gut – don't be afraid to look into things further. We have a lot of campaigns and when we start to robostamp things – that is when fraud gets through. We use people instead of machines for the gut check."

Fraud Executive,
Regional FI and
Credit Card Issuer

Account Takeover

ATO evolves with the market

Much like their law abiding counterparts, fraudsters enjoy adopting the newest gadgets to enter the payment world. Mobile wallets in particular offer unique opportunities for fraud rings built around POS card fraud, even as EMV reduces their window of opportunity for counterfeit cards. Because these rings tend to be geographically anchored, built around a network of runners and fences to acquire and liquidate stolen goods (respectively), transitioning to CNP fraud is not an easy option. CNP fraud requires both technical skill in confounding online merchant security measures and a geographically diverse network of reshippers to receive fraudulently purchased packages to avoid raising suspicion by repeatedly shipping to the same address.

By enabling the use of CNP credentials at physical stores, mobile wallets have provided a mechanism for POS fraud rings to make use of available credentials while maintaining their existing infrastructure. In some cases, they may need to take over fraud victims' accounts, subverting step-up authentication by diverting bank communication to a channel they control.

Seventy-five percent of issuers believe that ATO will become more problematic with the proliferation of mobile wallets (see Figure 13). This effect is augmented by the ongoing rollout of EMV, which has the dual effect of squeezing POS fraud rings out of their previous means of business and bringing waves of NFC-enabled terminals to storefronts, increasing the opportunity for use of mobile wallets.

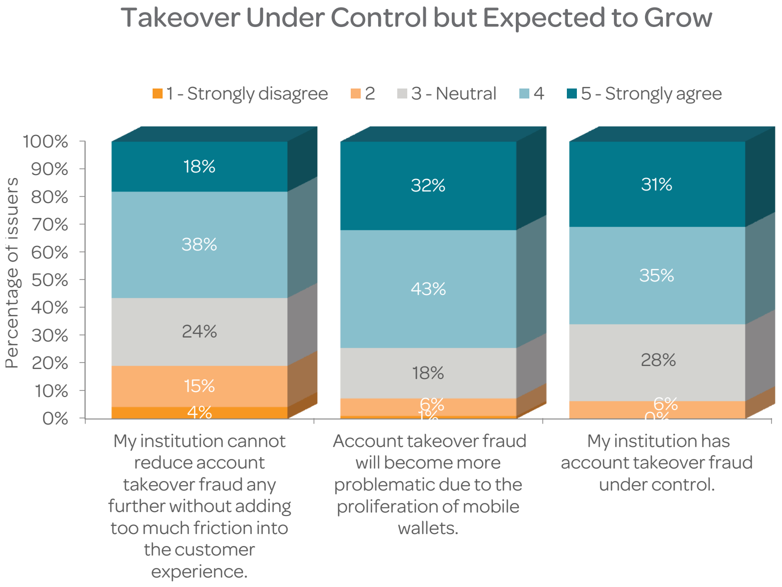

Takeover Under Control but Expected to Grow

Figure 13.Issuer Attitudes Toward Account Takeover

"We just introduced Apple Pay. Knock on wood, we have not had any significant fraud being very mindful of the mistakes made by early adopters. We use step-up on yellow path, have written tight rules for the use of Apple Pay, especially at Apple stores."

Fraud Executive, Regional FI and Credit Card Issuer

"It will be secure as long as we can partner with providers to get the level of detail to securely bind the device to the user. Integrating biometrics as well, but it all hinges on a strong initial registration process. Assuming this is all in place, I think that mobile wallets provide more of an opportunity than risk."

Fraud Executive, Large National FI and Credit Card Issuer

What makes this especially concerning is that, while more than half of issuers believe that they currently have ATO under control, 56% believe that they cannot reduce it any further without adding too much friction into the customer experience (see Figure 13). Over the long term, this balance can be maintained as defense tools' effectiveness improves at the same rate as those of fraud schemes, but it is a precarious position to be in when there are concerns about short-term spikes in fraud.

Without a doubt, what makes ATO so pernicious is that it confounds issuers' attempts to contact the legitimate accountholder, subverting many step-up authentication techniques used to verify questionable transactions. By directing all communication to channels they control, fraudsters are able to intercept calls, emails, and SMS alerts intended to alert cardholders to suspicious activity. With communication channels blocked, the fraudster is able to maintain control of the account for an extended period of time — draining all available funds or using it as a platform to open new accounts under their control. Consequently, it is no surprise that issuers listed this difficulty in communicating with the legitimate accountholder as the greatest obstacle in mitigating ATO with 47% of issuers ranking it as either the most or second most difficult challenge (see Figure 14).

Contacting the Legitimate Accountholder Is the Most Significant ATO Challenge

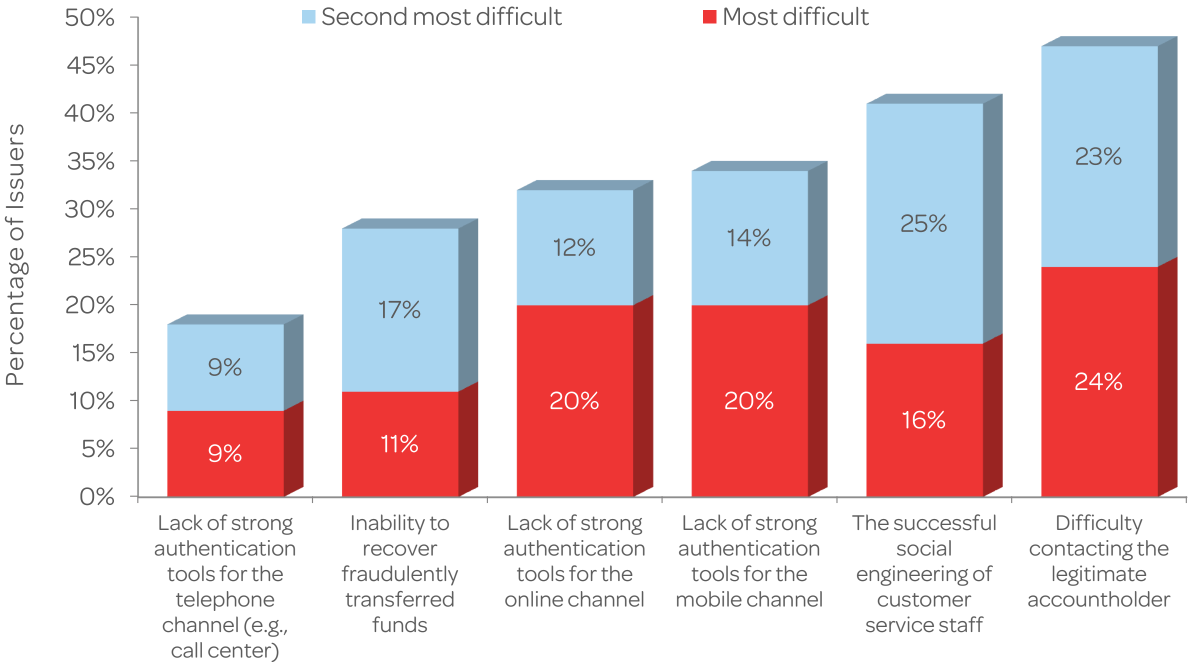
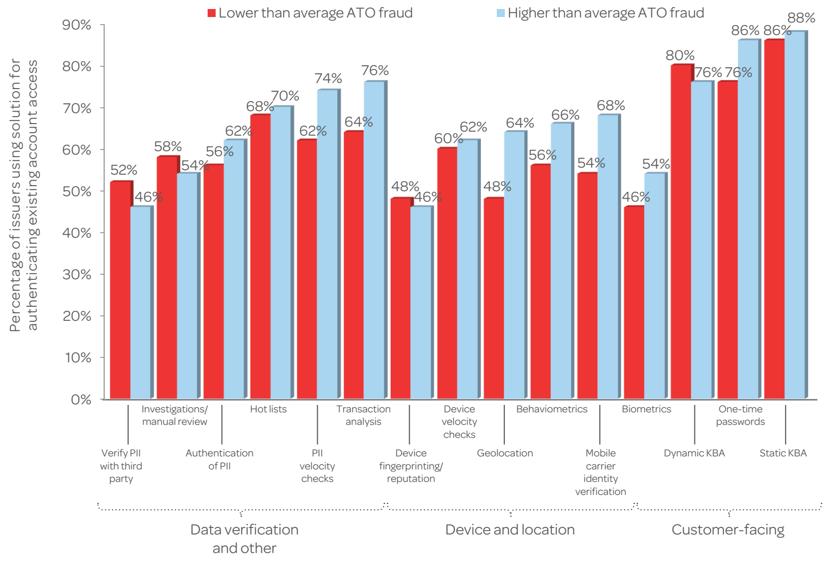


Figure 14.Challenges in Mitigating Account Takeovers

Under pressure: Social engineering the call center

To accomplish ATO, fraudsters will frequently target customer service representatives as the weakest link in the account access process. Recognizing this problem, 41% of issuers indicate that successful social engineering of customer service staff is either the most or second most difficult challenge in mitigating ATO (see Figure 14). CSRs are notorious for "rooting for" the customer — aiding customers who appear to be struggling at remembering security questions in an effort to maintain a positive customer experience. Add the desire to serve the customer with a lack of effective tools to verify the identity of a caller, and fraudsters are free to spin a tale that is convincing enough to justify access to the account.

Even if CSRs are trained to avoid social engineering, call center authentication frequently reverts to either static or dynamic KBA, asking questions that the fraudster may be able to answer with data they find on the black market or through their own research on the targeted cardholder. Moreover, CSRs have the ability to override fraud flags on risky transactions and account changes, allowing fraudsters to have essentially free rein on an account once they have convinced the CSR of their legitimacy.



Static KBA Is Closely Followed by One-Time Passwords and Dynamic KBA in Use Among Issuers for Authentication, Regardless of the Rate of ATO Experienced

Figure 15.Use of Tools for Authentication, Based on ATO Rate

"We got hit by a unique account takeover linked to data breaches, where they socially engineered customer service to add contact information to an account, but not request a card. They then went on to request credit line increases and added travel notifications. Expecting more of this to come. I've had experiences at other banks where the old rules just won't work here."

Fraud Executive,
Superregional FI and
Credit Card Issuer

"A lot of management around account takeover, even app fraud, is training the banker to recognize it. We have invested in both the call center and banking centers, ensuring that this piece is included during training. In the banking center it is annual, with some complimenting content throughout the year."

Operations Executive,
Regional FI and
Credit Card Issuer

As with application fraud, this is particularly a problem when working with affiliates. Just over half of issuers allowing accountholders to access accounts through affiliates' locations indicated that preventing ATO through this channel is very or extremely difficult, the highest proportion for any channel (see Figure 16). Since the employees of affiliates are outside the control of the issuer, it can be particularly difficult to ensure that they are properly vetting the customer for account access.

Takeover Through Affiliates' Locations Most Difficult to Detect

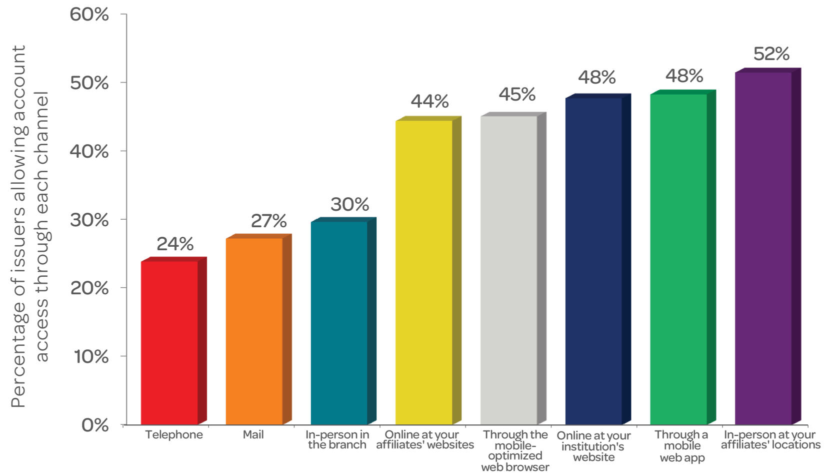


Figure 16.Difficulty of Detecting Account Takeover by Channel

Mitigating these challenges can be accomplished through a number of means. At a minimum, any change in contact information should be sent to both the original and revised contact. Ideally, use a channel that has been associated with successful communication in the past. This alert ought to contain both notification of the change and direction on how to notify the issuer in the event that this change was not authorized.

However, even a previously used communication channel is no guarantee of successfully reaching the legitimate cardholder. By preparing their fraud by arranging with the victim's mobile carrier to forward calls and texts to a different device, fraudsters can intercept both alerts without the victim's knowledge.

As a hedge against some of the aforementioned challenges, call centers should be hardened against fraud through security systems such as voice biometrics. Voice biometrics can more effectively identify legitimate cardholders, especially if there are previous call center interactions which can be used to establish a voice print. Even when the legitimate cardholder has not previously called the institution, voice biometrics can screen the caller to determine whether this individual has previously been associated with fraud. This flexibility, including the potential use across channels, contributes to about half of issuers using biometrics, regardless of whether or not they experience high rates of ATO (see Figure 15).

"We are starting to bring in some new tools in the call center space that will help us identify suspicious callers more effectively. We are also going to place some more effort on developing detection strategies for customer contact risk, both via phone and online. That is going to evolve and change over time."

Fraud Executive,
Large International FI and
Credit Card Issuer

Mobile carrier identity verification can provide more intelligence on devices that are new to the institution. By pulling records on phone ownership and billing records, mobile carriers can inform issuers whether the same PII is associated with the device and the card account. Because this information is not pulled from any interaction with the individual attempting to access the account, it is nearly impossible to falsify.

Hardening the online channel to benefit all

In an environment where credentials are being stolen in record numbers,[8] it is little surprise that the online channel is the most likely starting place for fraudsters during an ATO (see Figure 17). Between large-scale data breaches, the frequent reuse of passwords across websites, and banking Trojans that glean credentials as accountholders enter them, passwords are largely ineffective for preventing this type of fraud. Instead, issuers must turn to the same types of digital channel-specific tools that can serve them to such strong effect during the application process. Yet when dealing with a prospective or current customer, issuers must find that precarious balance between strong security and convenience.

Online Portals Are Favored for Initiating Takeovers, Followed by the Branch

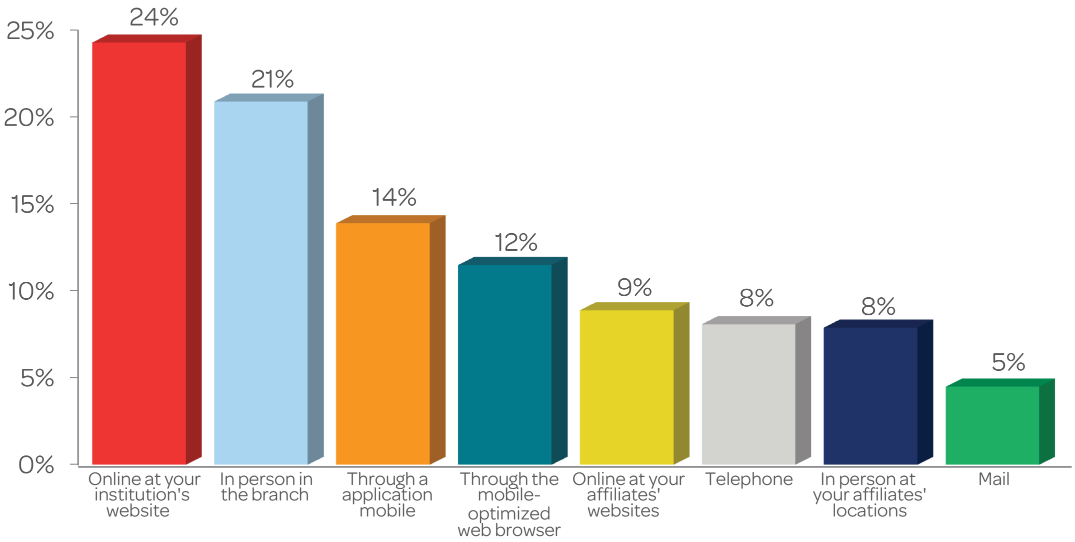


Figure 17. Channels Used to Initiate Account Takeovers

This need to balance convenience with security, along with the mix of channels targeted by fraudsters when committing ATO, affects the use of authentication solutions by issuers. While no solution is bulletproof, about half of issuers are using every tool that can be leveraged in the digital channel (see Figure 15). Digital channel-specific tools, whether new or established, in combination can be extremely effective and versatile. On their own, solutions such as behaviometrics and device fingerprinting/reputation can be utilized across device types and to prevent fraud under different circumstances. Their implementation is also necessary to address regulatory guidance on authentication controls.[9] Taken together though, the layering of these and other digital channel-specific solutions can be an extremely effective strategy to mitigate a spectrum of attacks initiated through the channel or to detect an attack initiated elsewhere.

Appropriate layering and implementation are crucial to balancing convenience with security, especially for issuers that have higher ATO losses and that are more likely to leverage more tools than their peers (see Figure 15). Controls for convenience and security should be implemented based on the degree of risk inherent to the transaction and in such a way that they cover each other's vulnerabilities. In the case of ATO, this would include not only high-risk payments or transfers, but also any changes to the contact information or credentials on an account, which precedes fraudsters' attempts to monetize the account during an ATO. Trading convenience for a more secure interaction during these moments is not only sound risk management, but also a truly consumer-oriented action as it puts the safety and the trust crucial to a financial services relationship first, exactly when it is most needed.

Sources

[1] http://www.forbes.com/sites/kellyphillipserb/2016/02/12/keeping-your-identity-your-refund-safe-from-fraudsters-at-tax-season, accessed March 11, 2016.

[2] http://www.creditcards.com/credit-card-news/credit-cards-history-1264.php, accessed November 23, 2015.

[3] 2014 Retail Point-of-Sale Payment Forecast: The Mobile Payment Square-Effect and Prepaid Card Popularity Drive Cash Down by 10%, Javelin Strategy & Research, May 2014.

[4] Online Retail Payments Forecast 2015, Javelin Strategy & Research, October 2015.

[5] 2015 Data Breach Fraud Impact Report, Javelin Strategy & Research, June 2015.

[6] U.S. "EMV-ification": The Growing Case for Contactless Cards, Javelin Strategy & Research, September 2015.

[7] 2015 Data Breach Fraud Impact Report, Javelin Strategy & Research, June 2015.

[8] http://www.reuters.com/article/2015/11/24/us-usa-cyberattack-russia-idUSKBN0TD2YN20151124, accessed November 24, 2015.

[9] Supplement to Authentication in an Internet Banking Environment, Federal Financial Institutions Examination Council, June 2011.

Methodology

In June 2015, LexisNexis retained Javelin to conduct a comprehensive research study on fraud encountered by U.S. card issuers. Javelin conducted an online survey comprising 100 risk and fraud decision-makers and influencers working at U.S. card issuers. The panel included issuers of all sizes in debit, credit, and prepaid card markets. The overall margin of sampling error is 19.75 percentage points at the 95% confidence interval; the margin of error is larger for subset respondents. Overall fraud loss data were weighted for number of cards issued of each type (credit, debit/prepaid), according to the industry distribution as recorded in the Nilson Report.

Executive qualitative interviews were also conducted with financial institutions to obtain their perspective on card fraud. A total of six interviews were conducted with risk and fraud executives.

For More Information

Call: 866.818.0265
Visit: lexisnexis.com/retail-ecommerce
Or email retailsolutions@lexisnexis.com

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions is a leader in providing essential information that helps customers across industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced analytics, LexisNexis Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information solutions for professional customers across industries.

About JAVELIN

JAVELIN, a division of Greenwich Associates, provides strategic insights into customer transactions, increasing sustainable profits for financial institutions, government, payments companies, merchants and other technology providers.

This document is for educational purposes only. LexisNexis does not warrant this document is complete or error-free. The opinions expressed by Javelin, and the quotes and opinions of the interviewed subjects, may not represent the opinions of LexisNexis.

LexisNexis® RISK SOLUTIONS | Financial Services