DIGITAL LENDING FRAUD

NOVEMBER 2017

Licensed by:

Intelligent Mobile Imaging
Mitek

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

ABOUT JAVELIN: Javelin Strategy & Research, a Greenwich Associates LLC company, provides strategic insights into customer transactions, increasing sustainable profits for financial institutions, government, payments companies, merchants and technology providers.

AUDIENCE: Financial institutions and other consumer lenders: digital channels, fraud, risk, and marketing departments; digital lending technology vendors; financial industry regulators; identity proofing technology vendors.

AUTHOR: Al Pascual, Senior Vice President, Head of Fraud & Security
Sean Sposito, Analyst, Cybersecurity
James Wilson, Research Specialist

CONTRIBUTORS: Kyle Marchini, Senior Analyst, Fraud Management
Sarah Miller, Research Manager – Custom Research & Operations

EDITOR: Chuck Ervin

PUBLICATION DATE: November 2017

OVERVIEW

The explosive adoption of the digital channel is changing the nature of lending. Consumers are coming to expect the kind of convenience and speed that a digital experience can deliver, and lenders are increasingly looking to oblige. Although many of the consumer benefits of digital lending are clear, certain complications related to fraud arise when lending goes digital. This is a function of the degree of separation and anonymity in the digital lending process. Building on these factors, today's fraudsters are relying on a diversified playbook of schemes and techniques to commit loan fraud in digital channels, including the use of synthetic identities, volumetric attacks, and technology designed to disguise their digital footprint. In this report, Javelin explores how these issues have come to unfold and the steps that lenders must take if they want to effectively resist this growing epidemic of digital lending fraud.

PRIMARY QUESTIONS

- What effect has the use of digital channels had on the lending space?
- How has fraud changed as a result of lending going digital?
- What are the technology factors affecting the risk of lending fraud in digital channels?
- What are the fraud risks specific to each type of loan product?
- How are different segments of consumers affected by digital lending fraud?
- What are the steps that FIs and other lenders can take to effectively prevent new account fraud?

EXECUTIVE SUMMARY

KEY FINDINGS

An improving economy and subsequent improvement in consumer creditworthiness is fueling the growth of lending and fraud. Credit scores are gradually improving with the economy. From 2015 to 2016, the average U.S. credit score rose four points from 669 to 673.[1] A higher average credit score means that more applicants can qualify for traditional loans. Besides lowering the bar to entry for consumers and making it easier for lenders to extend credit, it unfortunately also creates a broader set of useful identities for fraudsters to misuse.

Digital lending is introducing a degree of anonymity that is complicating fraud prevention. Although the benefits of providing digital loan applications to consumers are clear, certain complications that come with the process introduce a greater risk of fraud. The resources that banks and other traditional lenders use for in-person identity verification, such as government ID scanners, document scanners, and signature pads are not readily available in digital channels, and fraudsters are taking advantage of the anonymity.

Fraud losses from new loans have tripled in two years. The combined total losses associated with new fraudulent auto, personal, mortgage, and student loans have increased at an alarming pace. Overall, fraud losses from new loan accounts grew from $500 million to $1.1 billion, a 112 percent increase between 2014 and 2015. In 2016 they reached $1.5 billion, an increase over the prior year of 43 percent.

Smaller lenders run the risk of becoming attractive fraud targets as larger peers gain digital channel experience. Among the four largest U.S. FIs (Bank of America, Chase, Citibank, and Wells Fargo) customers used digital channels about two-thirds of the time at some point in the account opening process for checking, savings, and credit cards. That compares to 52%, 52%, and 66% for checking, savings, and credit cards, respectively, for smaller banks. Larger FIs are similarly ahead for other financial products, including lending products such as auto loans and mortgages. This means that smaller institutions are likely to be behind the curve when it comes to managing the risk of fraud during digital loan applications.

The weakness of credit reports for identifying fraud will only get worse. Credit reports are not necessarily updated in real time, and they might not contain information on all types of loans. A delay in reporting could mean that an underwriting decision could be made without the benefit of important data. In addition, because some alternative lenders might not run a credit report, meaning that fraudsters have more of an opportunity to avoid detection.

The combination of alternative lenders at times not using credit reports and fraudsters taking out multiple loans is costly. Consumers have been known to take advantage of alternative lenders and obtain multiple loans to get around restrictions, such as lending limits, without raising any red flags. This process is called "loan stacking," and it has greatly damaged the portfolio quality of many alternative lenders. Although some loan stacking might not constitute a crime, fraudsters could use this technique to fully exhaust a victim's creditworthiness before being detected.

Some loan products face an inherently lesser degree of fraud risk. Changes made in response to the mortgage crisis, such as doing away with stated and no-income loans and requiring income verification, have reduced the risk of mortgage fraud.[2] Borrower misrepresentation is on the rise in auto loans, but the nature of these loans helps insulate the market from more egregious cases of fraud. With products that don't typically appreciate in value and on which borrowers are highly dependent, outright misuse of third party's PII by a fraudster to obtain new auto loans is less likely than with other loan products.

Data breaches and digital ubiquity have given rise to synthetic identity. A fraudster's ability to be successful is first and foremost predicated on the use of an identity. Here there has been an evolution on the part of fraudsters as they take advantage of the anonymity of digital channels and the commoditized nature of personally identifiable information (PII). What has resulted is the synthetic identity: a sort of Frankenstein of identity information that can be used to circumvent traditional identity verification.

Faster application fraud attempts can overwhelm a lender's manual processes. Criminals are increasingly using decentralized botnets: groups of enslaved computers that can be used to fraudulently complete new application forms in large scale, taking advantage of stolen lists of information and automatically filling out applications in such volumes that it overwhelms the controls of lenders, especially when those controls have a manual element.

Millennials are more likely to be victims, but they aren't the most valuable lending fraud targets. Among Millennials, Gen Xers, and Baby Boomers, it is Millennials who are the most likely to have their identities used to open new accounts, but with their strong credit histories it is Baby Boomers that have the potential to be the most valuable to fraudsters.

RECOMMENDATIONS

Move beyond identity verification to identity proofing. Identity proofing is a vital aspect of the application process and should be tailored to the risks inherent in the channel, market, loan type, and threat environment. Relying on the simple validation of core PII elements to simultaneously comply with Customer Identification Program (CIP) requirements and manage fraud risk is no longer adequate to thwart fraudsters. Lenders must instead turn to a raft of new technologies and approaches to better manage the risk of new account fraud.

Implement an optimized identity-proofing workflow. To control for cost and customer experience while also managing fraud risk, lenders should use a thoughtful identity-proofing workflow that maximizes automation and relies on thoroughly reasoned decision logic for each loan product and channel. This will reduce unnecessary calls to costly services on applications. Lenders should also optimize this workflow to limit the use of manual processes by identifying fraud early in the proofing process.

Start by using an identity-proofing platform. A comprehensive identity-proofing platform that easily integrates with other tools to initiate calls to and consume inputs from various tools should be used. Other key features include machine learning and a diverse range of reporting options.

Beware of regulatory complications that could arise with certain solutions. Lenders should also be cognizant of the implications of the Fair Credit Reporting Act (FCRA) and whether a solution exposes them to non-compliance risk in how it is used, its output, and factors considered, etc.

Limit the use of knowledge-based authentication (KBA). Young applicants are more likely to have thin credit files and few public records, making identification through KBA difficult. And although a tool like KBA might be attractive for Baby Boomers because they have long-established credit and public profiles, lenders run the risk of using questions that fraudsters find easy to answer and good applicants find difficult to remember.

Streamline data entry to limit fraud and improve the experience. In cases where information on an applicant cannot be carried over from an existing financial relationship, tools that can prefill information should be integrated shortly after an individual initiates an application. These include document-scanning tools and solutions that populate information from other sources, like mobile network operators (MNOs).

Use shared intelligence to limit sophisticated fraud. Tools that use consortium data could benefit lenders by providing insights into how individual identity elements have been used for detection of synthetic identities. They can also determine whether new applications have been submitted between application and closing or whether a device has been used for known fraud elsewhere and can be flagged as soon as the application is begun.

AN ECONOMIC REBOUND

In 2008, the financial crisis devastated the U.S economy. Precipitated by mass defaults on subprime mortgages, the overall lending market took a major hit and the country entered a recession. Despite efforts to bolster the economy, including interest rates that fell precipitously, lenders tightened up on all loans. This was followed by new regulations (e.g., the Dodd- Frank Act) that were enacted specifically to prevent similar crises, which arguably made the lending market even less attractive to FIs and other lenders.

Eventually, as with the cyclical nature of most economies, things started to turn around. Since the trough of the Great Recession, the U.S. economy has been slowly but steadily recovering and growing. Jobless claims and unemployment levels have been consistently dropping, the Dow Jones broke the 20,000 barrier, and the Federal Reserve has deemed there to be enough economic improvement to justify multiple rate increases of the federal funds rate. Historically low interest rates have spurred the previously crippled lending economy. Lending to consumers has resumed, and despite the increased caution, lenders find themselves challenged by fraudsters also looking to benefit from the renewed economy.

A STORY OF CAPITAL AND CREDITWORTHINESS

By the fourth quarter of 2016, the U.S. reached a record $9.3 trillion in outstanding loans, a 5% increase from the year before. Total loans have grown consistently each year since 2010.[3] Several related factors have spurred the revival of lending in the U.S.: As the economy grew stronger, the balance sheets of FIs improved, and attracted by low interest rates and a slate of new lending options, consumers once again turned en masse to FIs and other lenders for loans.

A return of liquidity was another major factor that fueled renewed growth in the lending market. During the Great Recession, the investor market took a dive, depriving lenders of a tremendous amount of liquidity. Lenders relied on investors to buy loan pools and derivatives because they provided a constant source of funding for all types of credit products, including auto loans, cards, and mortgages. And this funding dried up enough to force banks to scale back on lending to consumers.

To help shore up the capital position of U.S. banks, the federal government provided injections of funds. Unfortunately, these "bailouts" did little to re-energize bank lending because FIs were hemorrhaging cash from underperforming loans. It wasn't until many of these loans were removed from their balance sheets, either through purchases by the Federal Reserve or ultimately from charge-offs, that traditional lenders became willing to extend credit significantly to consumers once again. The securitization market has rebounded, and investors are back to buying loans in the years since the recession, providing further motivation for U.S. lenders.[4]

When times are good for consumers, paying off their high interest rate debt can be a top priority. Because credit scores are partially based on the percentage of debt used, paying down revolving debts will increase credit scores. Credit scores in the U.S. have been rising with the economy. From 2015 to 2016, the average U.S. credit score rose four points from 669 to 673.[5] A higher average credit score means that more applicants can qualify for traditional loans. Besides lowering the bar to entry for consumers and making it easier for lenders to extend credit, it unfortunately also creates a broader set of useful identities for fraudsters to misuse.

Another large contributing factor to the increased availability of credit comes from the growth in alternative lenders. These new providers have been shaking up the lending market, catching the eye of investors and consumers alike. With boosted funding, many alternative lenders have grown their portfolios at exponential rates: From 2010 to 2014, the top 13 alternative lenders increased their total loans made by 700%.[6]

THE EVOLUTION OF LENDING

DIGITAL APPLICATIONS INTRODUCE TRADITIONAL LENDERS TO ANONYMITY

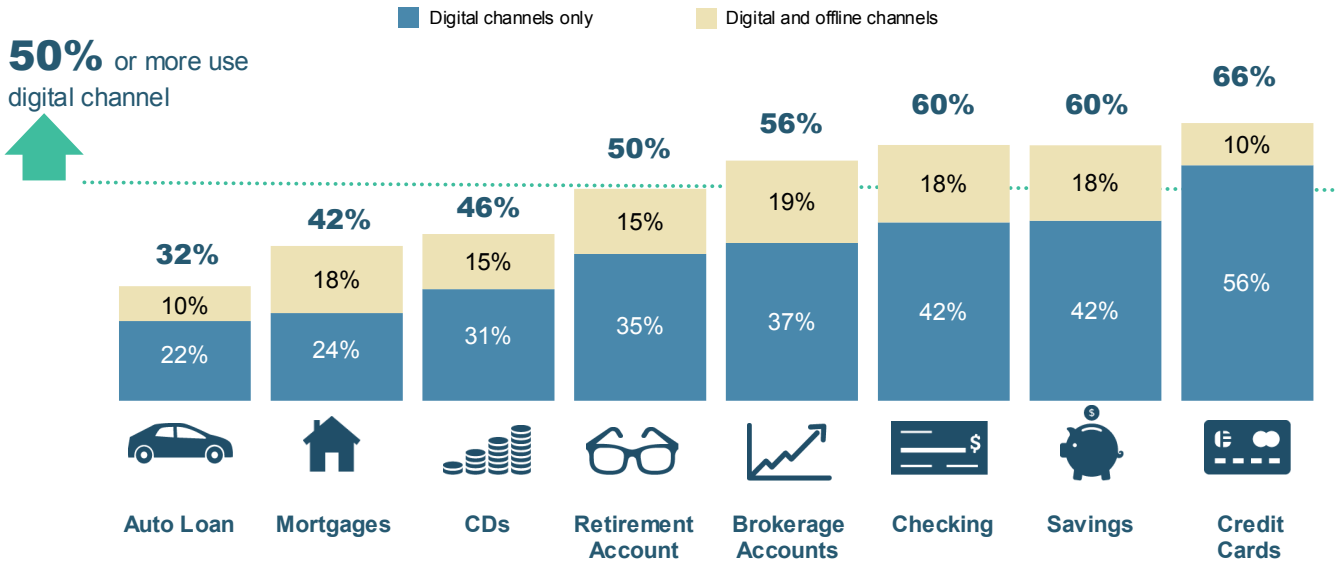
The explosive adoption of the digital channel is changing the nature of lending. Online banking usage rates have been growing steadily and are only slightly tapering off because the channel is becoming ubiquitous. Mobile banking is quickly catching up with online banking as the preferred channel.[7] Larger banks have made great strides in digital banking, and smaller banks are trying to keep up and cut costs. All banks want to make these channels profitable. For banks and other traditional lenders, that means they must figure out ways to sell products outside of their branches and storefronts. And that means adapting the application process to both online and mobile channels.

Although the benefits of providing digital loan applications to consumers are clear, the process introduces a greater risk of fraud. The resources that banks and other traditional lenders use for in-person identity verification — such as government ID scanners, document scanners, and signature pads — are not readily available in digital channels. Mobile devices now provide alternative ways to solve these problems so as to reduce risk and keep pace with alternative lenders that have emphasized the customer experience over controlling for fraud: for instance, integrating features like cameras to replace ID scanners and (at times) providing an end-to-end account opening process (see *Bringing Identity Proofing to Digital Lending*, pg. 16).

That said, the problem of offering an irresistible digital lending experience still evades FIs and other lenders. FIs have made a push for providing some products digitally but are relying on the branches to sell the most complex loans. Credit cards have the highest rates of digital account opening overall, with 66% of

Digital Channels Play Key Role in Account Opening

Figure 1: Accounts Opened Using Digital Channels, by Type of Account



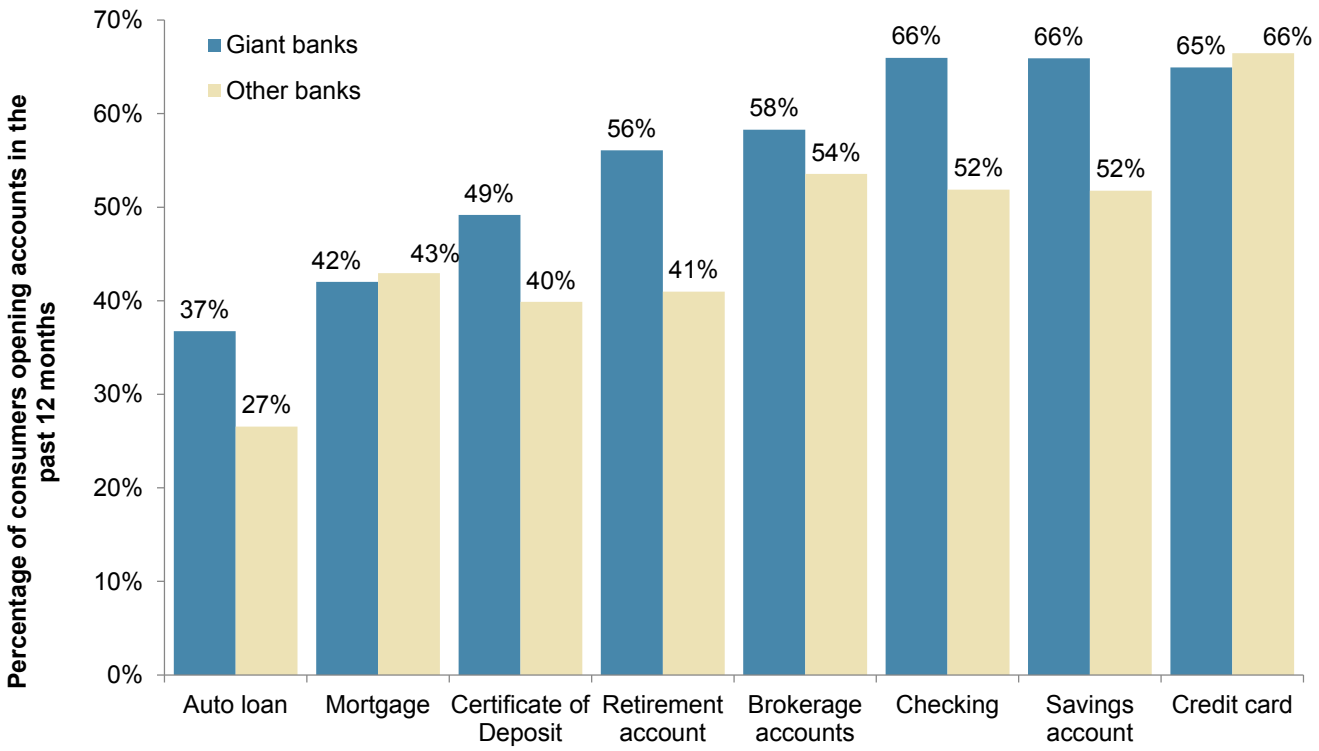
Source: Javelin Strategy & Research, 2017

customers using the digital channels at some point of the account opening process, followed by 60% for both savings and checking accounts. These numbers start to fall with loans, which require more documentation: Mortgages (42%) and auto loans (32%) are well below the credit card mark (Figure 1).

Larger FIs lead the pack when it comes to digital account opening. Among the four largest U.S. banks (Bank of America, Chase, Citibank, and Wells Fargo) customers used digital channels about two-thirds of the time at some point in the account-opening process for checking, savings, and credit card accounts. That compares to 52%, 52%, and 66% for checking, savings, and credit cards, respectively, for smaller banks. Among all accounts, the large banks maintain at least a 35% rate for digital channel usage, with auto loans being their lowest rate, at 37%. This is still significantly larger than the smaller banks, which only have a 27% rate for auto loans (Figure 2). This means that smaller institutions will probably be behind the curve when it comes to managing the risk of fraud across these digital channel applications.

Giant Banks Go Digital

Figure 2: Accounts Opened Using Digital Channels, by Bank Size and Type of Account



Source: Javelin Strategy & Research, 2017

ALTERNATIVE LENDERS AND THEIR PRACTICES

One advantage alternative lenders have touted over financial institutions is that they use data other than the standard credit check to make an underwriting decision.[8] FIs pull credit on most loan products in order to assess risk and to make required assurances to the parties that will ultimately end up with the loans being originated. Alternative lenders, however, began their lives under less scrutiny from investors and regulators. As a result, they had the latitude to be more creative and look at other customer characteristics to determine creditworthiness.

For instance, alternative lenders may consider longitudinal data on rent and utility bills as a way of discerning a borrower's viability. One alternative lender even lets consumers vouch for their friends to get a small personal loan. The aptly named firm Vouch will let applicants invite friends to cover portions of the loan in the case of default, almost like a co-signer. Through this non-traditional approach the underbanked can secure larger loans, freeing up their expenses for necessities.[9] By determining creditworthiness in unconventional ways, alternative lenders have been able to capitalize on groups of people ignored by FIs.

It is not all good news for alternative lenders, though, because they have faced difficulties associated with their quick approvals, including poor credit quality and excessive fraud. Faster approval times can be a great perk and can be very appealing to a credit-hungry consumer. But they can be problematic when consumers want to take out multiple loans at the same time unbeknownst to the lender or in some reported cases, with the cooperation of lenders.[10] And as alternative lenders have extended their offerings beyond personal loans and to other financial products, such as mortgages, weak fraud controls have the potential to lead to outsized losses.

To backtrack a bit, traditional lenders look at all of a consumer's outstanding debt to see how leveraged they are when making a credit decision. Lenders can obtain the customer's traditional borrowing history with available balances through a credit check. Credit reports, though, are not necessarily updated in real time, and they might not contain information on all types of loans. This means that any underwriting decision could be made without the benefit for important data. In addition, by not running a credit report, fraudsters can take out multiple loans and go undetected.

The combination of alternative lenders at times not using credit reports and fraudsters taking out multiple loans is costly. Consumers have been known to take advantage of alternative lenders and obtain multiple loans to get around restrictions, such as lending limits, without raising any red flags. This process is called "loan stacking," and it has greatly damaged the portfolio quality of many alternative lenders. Although some loan stacking might not constitute a crime, fraudsters have also been known to partake in this technique to fully exhaust a victim's creditworthiness before being detected.

As with any nascent market, alternative lenders have grown with the benefit of having relatively few regulations. Because they are not subjected to the same regulations and costs that are associated with abiding by those regulations, alternative lenders have had a competitive edge over FIs in the digital space. However, alternative lenders' rapid growth has caught the eye of the U.S. Treasury.

The Treasury's concerns stem from these lenders' level of transparency in the underwriting process. Since alternative lenders use big data to approve loans, applicants do not always know why they are being rejected.[11] This can be especially problematic when customers are turned down for a reason that might appear discriminatory. For instance, some lenders look at qualitative consumer data to determine long-term income projections. A large piece to that puzzle favors graduates of Ivy League universities, admission to which largely favors applicants from affluent families. Whether this constitutes discrimination is up to debate, but the Treasury is pushing for greater detail in letting consumers know why they are rejected for a loan.

DIGITAL LENDING FRAUD TRENDS

Banking customers are increasingly looking past the branch when it comes to opening an account. However, loan officers cannot look into the face of borrowers during a digital channel application, checking the color of their eyes and the shapes of their faces against a driver's license. Instead, FIs must take stock of a borrower's digital identity: IP addresses and device fingerprints, among other vital pieces of virtual information. Fraudsters have taken advantage of the anonymity that virtual channels provide and the tools FIs have come to rely upon, learning their weaknesses and creating a playbook to exploit them.

Today's fraudsters are relying on an increasingly diversified playbook of schemes designed to take advantage of vulnerabilities in the digital application process. Beyond using the knowledge that alternative lenders are easy targets for loan stacking, fraudsters have numerous options for broadly misusing identity and technology to fool FIs and other lenders, including synthetic identity fraud, volumetric attacks, and technology to disguise their digital footprint. All of this has helped make fraudsters effective adversaries.

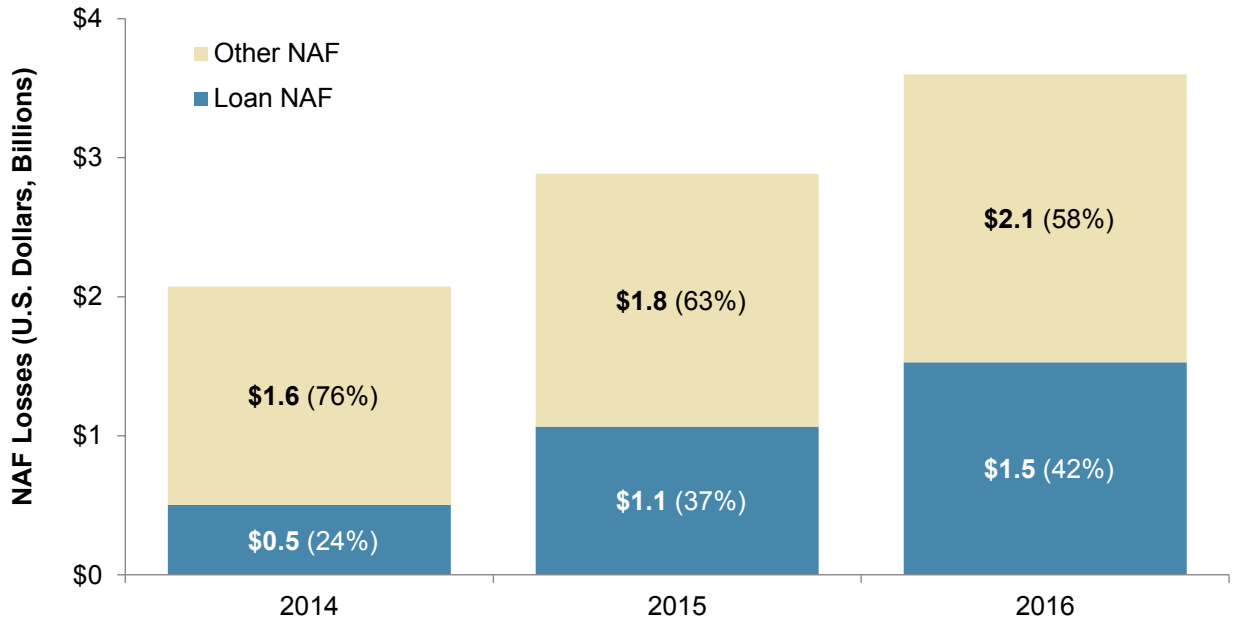
NEW ACCOUNT FRAUD IS ON THE RISE

Fraudsters have had more to be happy about as losses from lending fraud have increased significantly since 2014. When new account fraud (NAF) losses are categorized by account type, the trend and implications become clearer:

- **Both lending and non-lending new account fraud grew.** But it was the former that shot up at an alarming pace. Overall, fraud losses from new loan accounts grew 112 percent between 2014 and 2015, and they increased another 43 percent in 2016 (Figure 3).

New Account Fraud Continues to Rise

Figure 3: Fraud Losses (U.S. Dollars, Billions)



Source: Javelin Strategy & Research, 2017

- **The rate of growth has slowed, but it is still strong.** That means in order to continue to make margins, criminals are becoming more creative in their schemes and with whom they target. Their approaches, whether they are automated or based on the ingenuity of a single group, represent an evolving landscape of fraud. Crooks are adapting as sophisticated lenders become more aware of underground marketplaces and the types of data bought and sold on the dark web and the deep web, improving their tools and probably broadening their scope of targets to include smaller lenders who are new entrants to the digital lending space.

TECHNOLOGY AND PRODUCT FACTORS INFLUENCING DIGITAL LENDING FRAUD GROWTH

Criminal creativity has acutely manifested itself in new account fraud, a crime affected by the shortcomings inherent in most digital loan applications. Vulnerabilities and motivators include:

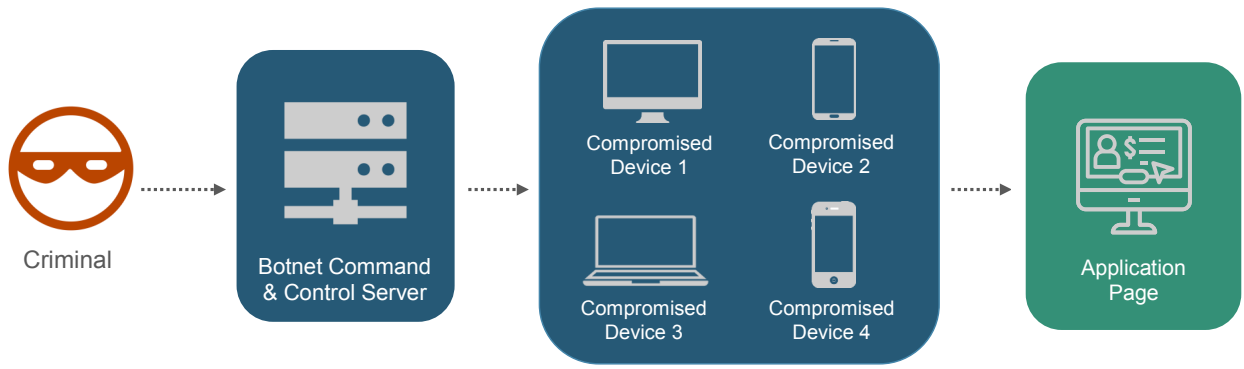
- **Data-validation solutions** that are prone to errors due to duplicated, old, or incorrectly entered entries that allow synthetic identities to hide within the noise. These same solutions have also been abused by crooks to facilitate NAF. [12]
- **Data breaches** are so extensive that they include even people's most personal details, such as Social Security numbers, which are used to fill out loan applications. As a result, threat intelligence vendors and FI employees are identifying stolen information as it moves across the dark web and the deep web. In many cases, unannounced to the operators of these underground forums, FIs are surveilling the company data that criminals are advertising for sale.[13]
- **The advent of EMV** chip cards has encouraged fraud rings to think beyond brick-and-mortar store counters. New account fraud, in fact, is incredibly attractive to these groups in light of payment card innovations. Because, rather than going through the hassle of taking over an account, these crooks can simply control a new one. With the viability of counterfeiting no longer in the cards, one of their next best options is to apply for new cards and other loan products with fraudulently obtained or outright false information.

From a technology perspective, criminals are clearly taking advantage of the decentralized nature of botnets. These groups of enslaved computers are being put to the task of automating volumetric attacks that both obscure a criminal organization's locations, with the help of other technologies such as virtual machines, and provide them with additional resources (Figure 4).

In one example, a private botnet called GameOver Zeus — so named because of the devastating nature of the banking Trojan it spread — reportedly controlled roughly 300,000 computers across the globe.[14] In summer 2014, the FBI, in concert with private industry, "took over" the botnet and charged its administrator. In a statement, an agency spokesman said the global botnet had

Criminals Are Monetizing Stolen Data Quickly

Figure 4: Bots Allow for Exponentially More Fraud Applications



Source: Javelin Strategy & Research, 2017

"stolen millions from businesses and consumers as well as a complex ransomware scheme that secretly encrypted hard drives and then demanded payments for giving users access to their own files and data."

In the context of lending and account opening, such tools can be used to fraudulently complete new application forms at large scale, taking advantage of stolen lists of information and automatically filling out applications in such volumes that it overwhelms the controls of lenders. This scheme is especially effective when those controls have a manual element.

Although it is true that accepting digital channel applications can be a significant risk factor, some loan types are more or less prone to new account fraud because of factors inherent to the products.

- **Auto Loans:** Borrower misrepresentation is on the rise in auto loans, but the nature of these loans helps insulate the market from more egregious cases of fraud.[15] With products that don't typically appreciate in value and on which borrowers are highly dependent, outright misuse of third party's PII by a fraudster to obtain new auto loans is less likely than with other loan products.
- **Mortgage Loans:** Changes made in response to the mortgage crisis have largely stemmed fraud schemes that were once commonplace, including falsified incomes and straw borrowers. Such changes included doing away with stated and no-income loans and requiring income verification.[16]
- **Personal Loans:** Not requiring collateral, FIs and alternative lenders are offering up a dream product for criminals. These loans are perfect for high-volume digital application attempts, especially when there is little in the way of documentation requested from the borrower.
- **Student Loans:** In these cases lenders report that fraud can be well controlled by distributing the funds directly to the educational institution or to a student address on file with their educational institution. Instead, fraud tends to arise from cases where students submit their parents or guardians as co-borrowers without their knowledge – in which case, digital channel applications will only make this process easier.

WHAT'S IN A NAME?

A fraudster's ability to be successful is first and foremost predicated on the use of an identity. Fraudsters' tactics have evolved as they take advantage of the anonymity of digital channels and the commoditized nature of personally identifiable information (PII). Broadly, the types of identities used to commit new account fraud can be divided into two main categories:

- **True name**: Enabled by the wealth of PII available to them through both the dark web and simple searches of the Internet, fraudsters will employ a curated collection of data about an individual consumer to subsequently convince a lender that they are in fact a legitimate applicant.
- **Synthetic identity** does not imitate a true identity. Rather, core identity elements can represent a mix of real and fake PII, including that of children. These core elements — which are central to a customer identification program — specifically include the name, Social Security number, and date of birth.

Synthetic identity schemes are particularly insidious. The data points they involve might be individually valid or new to the system. That makes them especially difficult for FIs to flag as false. Fraudsters will go to great lengths to bolster the value and apparent legitimacy of these identities, such as by adding them as authorized users to the accounts of legitimate consumers by way of "work from home" schemes. Additionally, because no single victim can step forward, fraudsters are better able to use these patchwork identities for a valuable web of networked accounts.

HOW GENERATIONAL DIFFERENCES INFLUENCE FRAUD RISK

Consumers in different generational segments display distinct behavioral patterns that directly affect their risk of having their identities used in lending fraud. Millennials tend to be more active online, whereas Baby Boomers are more cautious about the security of their finances, including where they share information. Gen Xers end up being in the middle of most characteristic traits, sharing qualities with the other two groups. And for lenders and

fraudsters alike, there are other innate qualities that affect each generation's risk of lending origination fraud.

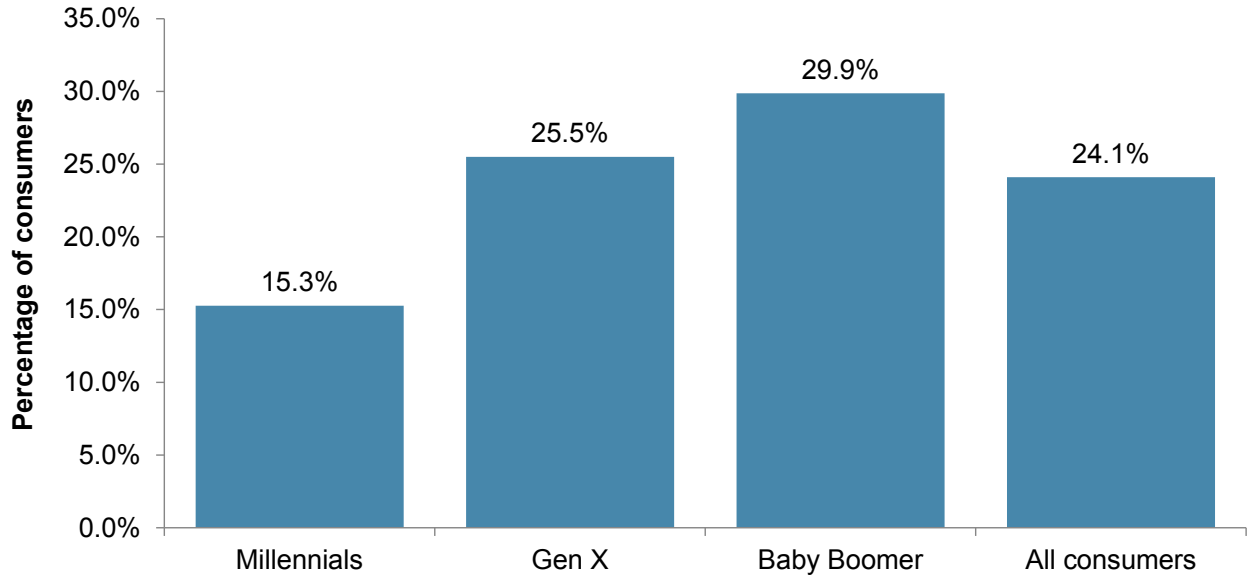
New-to-borrowing Millennials generally have fewer financial accounts than older consumers. What that means for fraudsters is that they do not have as many opportunities for existing-account fraud (EAF) or account takeover (ATO) fraud. Therefore, Millennials are more likely to be victims of new account fraud (NAF), (Figure 6). Furthermore, Millennials tend to be more blasé about monitoring fraud. By contrast, Millennials are great about online security hygiene. They are better about maintaining privacy settings on online profiles and updating antivirus and malware. As goods as Millennials are about digital security, though, they are just as bad about physical security habits. They are more likely to leave sensitive documents out, making them vulnerable to familiar fraud – or fraud committed by someone whom the victim personally knows.[17]

Millennials are some of the first adopters when it comes to the digital world. Account opening should be an obvious fit for this demographic, but common identification approaches introduce roadblocks. For example, knowledge-based authentication (KBA) may be used to identify applicants in these cases. Young applicants are more likely to have thin credit files and few public records, making identification through KBA difficult.

Gen Xers naturally share qualities with both Millennials and Baby Boomers. Gen Xers are often first adopters with new technology, much like Millennials, but they also monitor for fraud at a higher rate just like Baby Boomers. Because they share similar qualities with both generations, they tend to be the Goldilocks of segmentation. Gen Xers have an NAF incident rate in the past six years of 1.3% for loan products, which is lower than Millennials and higher than Baby Boomers (Figure 6). They also are better about owning ID protection services than Millennials, at a rate of 26% vs. 15%, but still lower than Baby Boomers' rate of 30% (Figure 5).

Baby Boomers Most Likely to Turn to Identity Protection Services

Figure 5. Subscription Rates for Identity Protection Services, by Generation



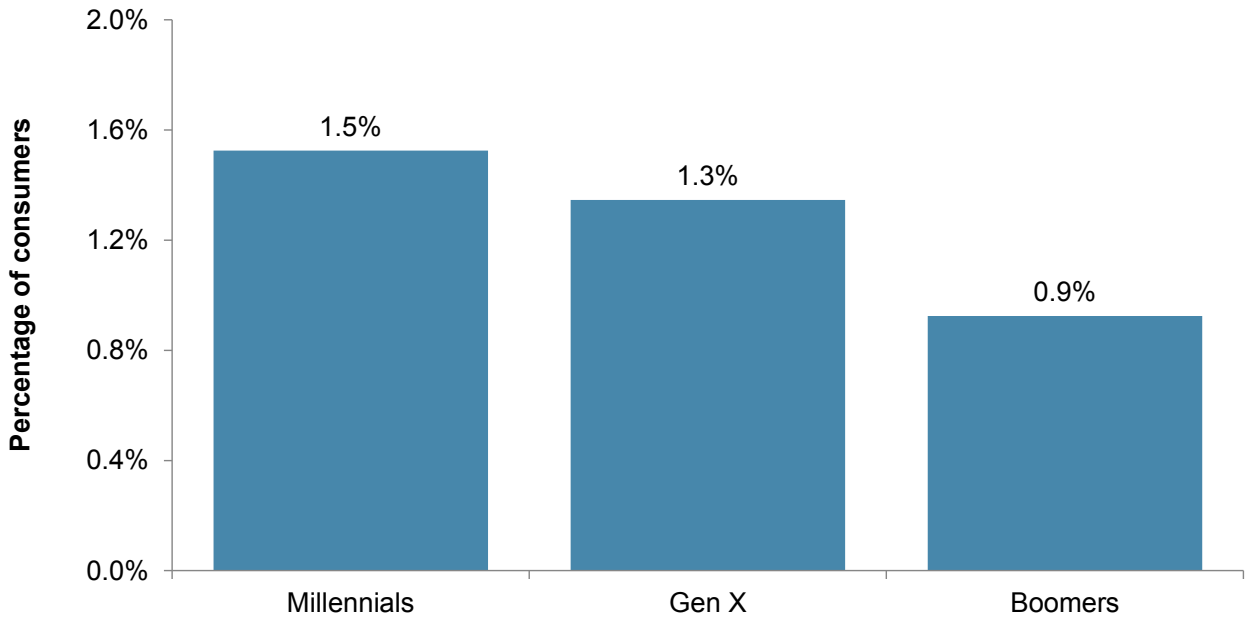
Source: Javelin Strategy & Research, 2017

From a credit standpoint during the Great Recession, Gen Xers were hit the hardest. On average they lost 45% of their median net worth.[18] Gen Xers had more "skin in the game" than Millennials, who were just starting their careers. Compared to Baby Boomers, Gen Xers had relatively shallow credit histories at the time. Because they were likely to be living in the first homes they ever purchased when the market collapsed, Gen Xers' credit scores were disproportionately affected. As a result, this generation is still recovering from the crash, and fraudsters are finding their credit less useful. On the flip side, Gen Xers are in the prime earning years. As a generation they made up nearly half (42%) of all personal income in 2015.[19]

Baby Boomers tend to be more nervous about potential threats, as they should be. Baby Boomers are very attractive to fraudsters because of their relatively gleaming credit scores. Their average credit score is 700, whereas Gen X and Millennials have 665 and 634 average scores, respectively.[20] Because credit scores factor in longitudinal data when assessing creditworthiness, average credit scores are directly correlated with age. A higher credit score makes Baby Boomers far more appealing to fraudsters for NAF. That is because their strong creditworthiness will allow fraudsters to take out larger loans. And although a tool like KBA might be attractive for this segment because they have long established credit and public profiles, lenders run the risk of using questions that fraudsters find easier to answer and that good applicants find difficult to remember. So unbeknownst to the lenders, who might believe that they are lending to responsible and financially fit Baby Boomers, they might in fact be extending the credit to fraudsters.

Millennials Are Prone to New Account Fraud

Figure 6: NAF Incident Rate for Loan Products, Past Six Years



Source: Javelin Strategy & Research, 2017

BRINGING IDENTITY PROOFING TO DIGITAL LENDING

Identity proofing is a vital aspect of the application process and should be tailored to the risks inherent in the channel, market, loan type, and threat environment. Relying on the simple validation of core PII elements to simultaneously comply with CIP requirements and manage fraud risk is no longer adequate for thwarting fraudsters. Lenders must instead evolve their identity proofing capabilities by turning to a raft of new technologies and approaches to better manage the risk of new account fraud.

Cost and customer experience implications dictate that a lender be judicious with its use of different identity verification and authentication tools. This should manifest in the creation of a thoughtful identity-proofing workflow that maximizes automation, relies on thoroughly reasoned decision logic for each loan product and channel, and minimizes unnecessary calls to costly services on applications. Lenders should also optimize this workflow to limit the use of manual processes by identifying fraud early in the proofing process. Below is a model workflow that lenders can use to establish a robust identity proofing capability.

BEFORE IT STARTS

A comprehensive identity-proofing platform that easily integrates with other tools to initiate calls to and consume inputs from various tools should be in use.

- Any platform should allow the creation of custom rules and workflows for different loan products and channels and offer a sufficiently wide scoring band, allowing for granular customization.[21]
- The inclusion of machine-learning capabilities to improve efficiency and accuracy in scoring applicants for fraud is critical, especially where application volumes have the potential to be significant, and reporting should be flexible to provide immediate visibility.
- Scores should be calculated and used to influence the workflow at each step in the application process.
- Lenders should also be cognizant of the implications of the Fair Credit Reporting Act (FCRA) and know whether a solution exposes them to non-compliance risk in how it is used, its output, and factors considered, etc.

KNOW YOUR ENEMY FROM THE BEGINNING

Device and behavioral analyses should be in place to passively assess risk from the beginning of the session:

- Drawing on device fingerprinting, providers that can offer a broad view into devices' reputations from many institutions can further help to clarify whether a particular device being used to initiate the application is suspect.
- Lenders have a variety of approaches to assess the behavior of the applicant and identify fraudsters or bots, including being able to analyze and take action on how an applicant uses the input device, provided by vendors such as BioCatch and SecuredTouch. Lenders can also act on how an applicant interacts with different elements of the session, as provided by vendors such as NuData Security, or even consider the cognitive implications of how applicants respond to different fields in the application itself, a capability unique to Neuro-ID.

STREAMLINE DATA ENTRY

In cases where information about an applicant cannot be carried over from an existing financial relationship, tools that can prefill information should be integrated shortly after an individual initiates an application:

- Document-scanning tools or solutions that populate information from other sources, like those offered by Payfone, should be integrated early because they can help streamline the process for legitimate applicants by prefilling common data fields.

- Each approach has its benefits: ID scanning creates a burden of proof on the applicant to offer a valid document that can be visually inspected. Using other data sources to prepopulate applicant data allows lenders to benefit from the identity verification and tenure of accounts managed by a third party, such as a mobile network operator (MNO).
- Prefilling is especially useful for mobile channels, either app or web, because manually entering information is tedious for applicants in either case.

ASSESS THE PROVIDED DATA

The ability to not only verify data provided and gain insight into the history of that data is critical in avoiding fraud.

- Any internal resources should be used first, including hotlists that might indicate whether an applicant or an element of his or her PII has been used in previous cases of fraud.
- During this stage, FIs can verify that the PII provided matches a single identity and use data from MNOs to verify ownership and ascertain the status of the mobile number, such as whether it is being ported.
- Using consortium data, or data from across a network of participating lenders, can be used to increase the odds of detecting synthetic identity fraud or to spot loan stacking, a key feature offered by TransUnion.
- Financial account verification, from providers such as Yodlee, should be used in cases where a fraudulent or mule account could be involved.
- FIs should consider not just the totality of an applicant's identity but also the history of each data point through a consortium relationship to establish whether any elements of that applicant's identity were involved with fraud elsewhere, as supported by ID Analytics.

MAKE ONE LAST ATTEMPT BEFORE GOING MANUAL

Manual reviews of loan applications can be costly and can introduce delays in what is supposed to be a fast, smooth customer experience. Before passing a poorly scoring application to a member of the fraud team, consider using a digital tool to reduce risk.

- The verification of identity documents can instituted at this step, if not done earlier or if additional documentation is needed, through the use of a document scanning tool, such as those from AU10TIX, Jumio, or Mitek.
- If the use of an SMS, voice, or email one-time password is warranted, be certain that the contact information on file belongs to the applicant in question either through the use of MNO data or a solution such as Emailage — again if verification was not performed earlier.

INSTITUTE MANUAL REVIEWS AS A LAST RESORT

If the fraud risk is still unclear, lenders can choose to route the application for a manual review. Given the considerable cost, this should occur after creditworthiness has been established.

- Introduce checklists for any potential red flags that cannot be easily discerned in an automated fashion, so that a fraud analyst or investigator can better decide where to focus his or her efforts and subsequently limit the use of costly tools.
- Checklists can even be used at other points in the origination process to identify fraud, such as during the review of documentation by processors or underwriters.
- During a manual review, analysts or investigators might search public records, such as property ownership or professional licenses, or use approaches that are typically more expensive. These can include employment or tax verification or manually collecting and verifying identity, income, or employment documents.

ENDNOTES

1. http://www.experian.com/assets/live-credit-smart-2016/state-of-credit-infographic-2016.pdf, accessed August 12017.
2. https://www.bloomberg.com/news/articles/2017-05-10/auto-loan-fraud-is-soaring-in-a-parallel-to-the-housing-bubble, accessed November 6, 2017.
3. https://www.firstdata.com/en_us/insights/first-data-us-financial-institution-quarterly-newsletter.html, accessed July 25, 2017.
4. https://www.economist.com/news/finance-and-economics/21593424-much-maligned-financial-innovation-early-stages-comeback-back, accessed November 1, 2017.
5. http://www.experian.com/assets/live-credit-smart-2016/state-of-credit-infographic-2016.pdf, accessed August 10, 2017.
6. https://www.americanbanker.com/news/marketplace-lending-grew-by-700-in-four-years-report, accessed July 25, 2017.
7. **Online Banking Forecast 2016: Optimizing Online Banking in a Mobile Era**, Javelin Strategy & Research, February 2016.
8. https://www.forbes.com/sites/nickclements/2015/04/21/5-reasons-new-lenders-are-ignoring-fico-credit-scores/#4db0231c2838, accessed August 10, 2017.
9. https://www.americanbanker.com/news/with-a-little-help-friends-vouch-for-borrowers-in-new-loan-model, accessed July 24, 2017.
10. https://www.bloomberg.com/news/features/2016-08-18/how-lending-club-s-biggest-fanboy-uncovered-shady-loans, accessed November 1, 2017.
11. http://www.pymnts.com/news/b2b-payments/2016/treasury-alternative-marketplace-lending-regulation-reclassify-small-business-consumer-loans/, accessed November 1, 2017.
12. https://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/, accessed November 1, 2017.
13. **2017 Data Breach Fraud Impact Report: Going Undercover and Recovering Data**, Javelin Strategy & Research, June 2017.
14. https://www.bloomberg.com/news/features/2015-06-18/the-hunt-for-the-financial-industry-s-most-wanted-hacker, accessed November 1, 2017.
15. https://www.bloomberg.com/news/articles/2017-05-10/auto-loan-fraud-is-soaring-in-a-parallel-to-the-housing-bubble, accessed November 6, 2017.
16. https://www.fanniemae.com/content/faq/borrower-income-verification-faqs.pdf, accessed November 6, 2017.
17. **2015 Identity Fraud Report: Protecting Vulnerable Populations**, Javelin Strategy & Research, February 2015.
18. https://www.cnbc.com/id/100744664, accessed August 10, 2017.
19. **Wealth Management In a Mobile-First Era**, Javelin Strategy & Research, December 2016.
20. http://www.experian.com/assets/live-credit-smart-2016/state-of-credit-infographic-2016.pdf, accessed August 10, 2017.
21. **2017 Identity Proofing Platform Scorecard**, Javelin Strategy & Research, September 2017.

CITED JAVELIN RESEARCH

Online Banking Forecast 2016: Optimizing Online Banking in a Mobile Era
February 2016
Online banking has been far and away the most vital touchpoint in an FI's relationship with its customers for the past decade. But the rapid proliferation of mobile banking has irrevocably shifted consumers' expectations around interaction with their primary financial institution: The chore of financial management is now implanted in our everyday lives, wherever we go. The trend toward mobile leaves digital strategists with an important question: Where does online banking fit? FIs looking to preserve the utility of online banking for an increasingly mobile audience must move beyond thinking about it as a transaction processor and instead prioritize features that highlight the characteristics unique to the online experience on PCs and laptops.

2017 Data Breach Fraud Impact Report: Going Undercover and Recovering Data
June 2017
In 2016, FIs were more vigilant about notifying their customers of fraud than ever before. That is the result of several contributing factors, not the least of which are new processes and increasing use of better technology. One of the most oft-discussed reasons for FIs increasing alertness, however, is their growing attention to online criminal communities. Whether FIs are interacting with criminals directly through their internal teams or receiving alerts from vendors about potential customer data being traded on underground forums, they are increasingly protecting customers through their use of subterfuge. This report explores this process, the motivation for FIs, and the thorny issues that can occur when FIs go undercover.

2015 Identity Fraud Report: Protecting Vulnerable Populations
February 2015
In 2014, 12.7 million consumers experienced identity fraud – a decline of 3% from the near record high of 13.1 million in 2013. A series of extraordinary responses to high-profile data breaches contributed heavily to this decline. In addition to exploring the drivers of fraud for all consumers, Javelin specifically examined military personnel, seniors and students to understand how their attitudes and behaviors relate to the fraud experienced by each of these segments. Javelin's "2015 Identity Fraud Report" provides a comprehensive analysis of fraud trends in order to inform consumers, financial institutions and businesses on the most effective means of fraud prevention, detection and resolution.

Wealth Management In a Mobile-First Era
December 2016
A growing number of so-called robo investment firms, fintech innovators, and bank partnerships is rushing to refine a cost-effective business model for investment services in a digital-first era. The challenges are numerous, starting with how to tempt today's affluent Gen X, Baby Boomer, and female investors to try untested upstarts while also grooming tomorrow's Gen Y banking customers who aren't yet rich. The outcome will be shaped by how well financial institutions incorporate robo capabilities in three categories: digital banking insights, robo advising and investing, and personalized "robo writing." Together, these services and players can build on Javelin's Financial Journey Model, usher in new ways to coach customers, simplify investment decisions, counter anxiety in volatile times — and put banks and credit unions in a strong position when customers are ready to invest.

2017 Identity Proofing Platform Scorecard
September 2017
One of the foundational fraud challenges that an institution faces — identity proofing — must be tailored to the risks inherent in the channel, market, product type, scenario, and threat environment. In the complex financial ecosystem of 2017, a bifurcated model of identity verification and authentication fails to meet the needs of accountholders or financial institutions. Accordingly, a much more holistic approach is needed to take into account a richer array of context around the identity and behavior of the consumer. In this report, Javelin examines how FIs can best manage identity proofing across different key use cases and provides a guide for selecting the most effective identity proofing platform based on functionality, innovation, and the ability to tailor the product to the needs of the business.

METHODOLOGY

Consumer data in this report is based on information collected in a random-sample panel survey:

- November 2016 survey of 5,028 adult U.S. consumers. For questions answered by all 5,028 respondents, the maximum margin of sampling error is +/- 1.40 percentage points at the 95% confidence level.
- A panel of 10,768 consumers in an online survey conducted from June to July 2017. The margin of sampling error is ±0.94 percentage points at the 95% confidence level for questions answered by all respondents.
- A panel of 10,639 consumers in an online survey conducted in May 2016. The margin of sampling error is ±0.95 percentage points at the 95% confidence level for questions answered by all respondents.

Companies Mentioned	
AU10TIX	NuData Security
BioCatch	Payfone
Emailage	SecuredTouch
ID Analytics	TransUnion
Jumio	Yodlee
Mitek	