LexisNexis®
RISK SOLUTIONS

WHITE PAPER

Confronting fraud at the call center: new tactics and the tools to defend your business

AUGUST 2016

CONFRONTING FRAUD AT THE CALL CENTER

Mitigating fraud is a persistent challenge for many financial institutions. Since 2010, fraudsters have stolen +$112 billion from Financial Institutions and Services Firms, including $15 billion in 2015 alone.[1] Fraud schemes continue to shift and evolve, leaving your business fighting an enemy best characterized by a formidable trait: constant change. The implementation of EMV technology for payment cards has stymied fraudsters' success in Point-of-Sale Fraud and left them looking for other routes to quickly perpetrate fraud that delivers immediate results and high rates of return. Recent data breaches have provided fraudsters with an ample arsenal of Personally Identifiable Information (PII) from which to attempt Application Fraud and Account Takeover Fraud. These factors have created a perfect storm of opportunity for fraudsters and the storm is headed straight for your call center.

This overview delivers a look into recent fraud threats that specifically target financial institutions at the call center level and details key considerations to help prevent fraud and protect your business.

Dialing down to the perfect place to attempt fraud

Call centers create an ideal target for fraudsters. In a recent study, Pindrop Security estimated that in 2015, one in every 2,900 calls coming into large banks' call centers was fraudulent and among regional banks the number narrows to one in 700.[2] Due to the dramatic proliferation in the number of contact channels and real-time contact methods organizations have to account for and the intense focus on EMV technology implementation, fraud defenses at the call center level have been neglected in recent years. Much of the fraud that begins at the call center is difficult to trace directly back to the point of origination and often goes undetected until it reaches critical mass. Call centers are also unique because of the human element involved— call center agents are expected to deliver a consistently positive customer experience and simultaneously perform first-line fraud defense. That is a difficult balance to achieve in today's customer-centric environment, leaving financial institutions' call center security in the precarious position of being only as strong as their weakest customer service agent.

Fraudsters have taken notice and shifted their focus to the call center level. According to one study, 72% of financial institutions expect the call center fraud loss trend to continue on an upward trajectory due to the roll out of EMV[3]. The latest tactics feature a cunning combination that exploits advances in phone technology and good old-fashioned human error to successfully take over an account or fraudulently open a new account.

Social Engineering: This scheme has been fueled by the wealth of breached PII information available in the open market and the fraudsters end game is Application Fraud or Account Takeover Fraud. In 2015 alone, there were 13.1 million identity fraud victims.[4] Social Security Numbers, maiden names, passwords and key identity details are abundantly available to fraudsters. Data breaches provide fraudsters with a baseline identity profile of their victim. They use that information to persuade the call center agent to unwittingly give up more information to help further complete

the identity profile. In more harmful cases, the fraudsters utilize the data profile they already have to convince the call center agent they own the identity in question and gain seamless access to an account.

The amount of damage created by Social Engineering situations is confounding. One security organization estimated the average amount fraudsters could potentially steal after successful social engineering attempts was $7.6 million per bank in a 2014-2015 study. The updated numbers for 2016 place that number closer to $11 million per bank.[5] Fraudsters have a wealth of identity information to perpetrate infinite Social Engineering schemes and the problem is only in the nascent stages. A 2016 LexisNexis® study on fraud found that 41% of card issuers see social engineering at the call center level as a serious contributor to the rising numbers in Account Takeover Fraud.[6]

In 2015 alone, there were 13.1 million identity fraud victims.

Fraud committed via phone manipulation: Phone technologies have become more advanced, more affordable and readily available for fraud organizations to use to their advantage. Fraud organizations are harnessing phone technologies at alarming rates to proactively perpetrate fraud. The proliferation of mobile devices only amplifies the situation. 90% of the world population owns a mobile phone and one-third of digital transactions are done on a mobile device.[7] At the basic levels, fraudsters are utilizing interactive voice response (IVR) systems to complete initial reconnaissance to use for Application Fraud and Account Takeover Fraud. At more advanced levels, fraudsters are using phone spoofing, porting and forwarding to manipulate systems and people at financial institutions to intercept passwords in real time, takeover accounts, perform wire transfers and more. By manipulating phones, fraud organizations can inflict immediate damage and quickly move onto the next target, often before the fraud is ever detected.

End fraudsters' evasive techniques by escalating authentication

Fraudsters seem to have radically turned the playing field in their favor and $15 B in financial institution fraud losses in 2015 support that assumption. However, the game is not over yet and there are many best practices to consider in building a stronger, more fortified line of defense against these current call center fraud threats. Staying vigilant and implementing more versatile, risk-responsive authentication workflows can go a long way in protecting your business and promoting a frictionless interaction for legitimate customers.

Build Integrated, multi-layered authentication protocols: The most successful fraud prevention strategies begin with risk based, multi-factor authentication that integrates identity intelligence from several fronts. Combining risk and contact channel appropriate authentication methods such as knowledge-based authentication (KBA) with additional authentication measures like device and phone intelligence, fraud analytics or a one-time password can help uncover incomplete pieces of a fraudster's identity profile and quickly unravel an Application Fraud and Account Takeover Fraud attempt. Integrating authentication solutions to work in conjunction with each other is an important step to ensure the customer experience for legitimate customers is preserved while you expand fraud prevention tactics.

Increase Data Quality: Knowledge based authentication is only as strong as the identity intelligence your business uses to perform KBA. A recent survey showed 2/3 of the top 50 financial institutions still allowed a Social Security Number to be used as an authentication method.[8] Performing KBA with information that is readily available to fraudsters via recent breaches, social media sites or simple internet searches is ineffective and inefficient.

To perform adequate KBA you need access to enhanced identity intelligence that is built from multiple sources that are frequently updated. Utilizing robust data sources that aren't readily accessed by the public is a KBA essential. In a successful KBA scenario, asking the right questions, to the right person, at the right time, rivals getting the right answers. The best practice for KBA is an analytic-based solution that can create dynamic, risk-responsive questions in real time. Arming your customer service agents with an efficient and agile KBA system helps close information loopholes that could be manipulated by fraudsters and enables agents to truly focus on the customer experience.

Identify the device upfront: An additional layer of fraud protection can be accomplished by authenticating a device at the beginning of a customer interaction. Verifying the full device identity and location attributes can provide essential information that could be used to uncover a fraud attempt or flag an interaction for additional authentication protocols. In the case of the call center, understanding the device identity and location can help call center agents confirm the device belongs to the caller, detect call spoofing attempts and understand if any fraudulent or suspicious activity has been associated with the device. Device authentication is a behind-the-scenes authentication step that won't disrupt the customer experience. Choosing a device assessment solution that can verify the full device identity and location attributes across multiple device channels, including desktop and laptop computers, mobile phones, and tablets gives your business the most flexibility to implement a successful device authentication process.

Confirm the call source: Knowledge is power, especially when it comes to thwarting phone fraud schemes. Being able to quickly connect a phone to an identity and understand the legitimacy of that association is important. The source of phone and identity data should offer robust phones coverage and be continuously updated. After a connection between a phone and identity is confirmed, the status of the phone and the type of phone comes into play as a key defense against phone

schemes. Being able to identify that a phone has been ported and spotting patterns in porting frequency is crucial to mitigating a fraud attempt. Phone intelligence can also help fortify a one-time password security process by confirming the relationship between an identity and a phone and underscoring abnormalities in real time. Your phone solution should seamlessly integrate with additional security and authentication workflows to support faster decisioning and a friction-free experience for legitimate customers and transactions.

Add voice biometrics: Biometrics create a significant barrier for large scale fraud organizations to overcome because they are unique and not easily accessed or replicated. Voice biometrics create an additional level of authentication that, unlike fingerprints or facial recognition, easily translates to the call center level. Voice biometrics offer authentication versatility that can be applied across multiple access points, including mobile devices, online usage and call centers. An ideal voice biometric solution is designed to help promote a positive customer experience and prevent implementation delays and technology road blocks. Choosing a software-as-a-service voice biometric solution can give your business an efficient and streamlined way to augment authentication for high dollar or high risk transactions.

Answer the threat of call center fraud with agile authentication solutions

Organized fraudsters have an ever-accelerating arsenal of tools and data to commit crimes. Your organization is challenged to stay on constant alert. Multi-layered authentication helps your business create a defense strategy that leverages integrated prevention tools, advanced technology and current identity intelligence to proactively identify and mitigate Application Fraud and Account Takeover Fraud attempts at the call center level. The continuous evolution of the fraud game demands detection and prevention solutions that are flexible enough to operate from a risk-responsive basis to give your business the agility to adjust to shifting fraud schemes and defeat them as they develop.

LexisNexis offers industry-proven fraud, authentication and security solutions that combine leading identity intelligence with intuitive analytics to help your business prevent, detect and investigate fraud in critical interactions and transactions across the customer lifecycle. We would welcome the opportunity to discuss how we can help you build an integrated defense strategy that helps your business control fraud losses, optimize processes, reduce reputational risk and maximize the customer experience.

Sources:

1 Javelin Research, 2016 Identity Fraud Study: Fraud Hits an Inflection Point, February 2016.

2 Penny Crossman, "To Case the Joint, Press 1: Crooks Refocus on Bank Call Centers," American Banker, March 1, 2016, http://www.americanbanker.com.

3 Shirley Inscoe, "Contact Centers: the Fraud Enablement Channel," Aite, April, 2016.

4 Javelin Research, 2016 Identity Fraud Study: Fraud Hits an Inflection Point, February 2016.

5 Penny Crossman, "To Case the Joint, Press 1: Crooks Refocus on Bank Call Centers," American Banker, March 1, 2016, http://www.americanbanker.com.

6 LexisNexis® Card Issuer Fraud Study, April 2016.

7 According to ThreatMetrix Digital Identities, "Genuine Security for a Connected World" White Paper.

8 Javelin Research, 2015 Identity Fraud Study: Protecting Vulnerable Populations, 2015.

For more information call 866.858.7246 or visit
http://www.lexisnexis.com/risk/financial/fs-fraud-detection-prevention.aspx

LexisNexis® RISK SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government assess, predict, and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide 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 and analytics for professional and business customers across industries.