TABLE OF CONTENTS
INTRODUCTION .............................................................................................................................................. 3
CONTACT CENTER IN THE CROSSHAIRS.......................................................................................................... 4
WAYS AND MEANS.................................................................................................................................... 4
MITIGATING CONTACT CENTER FRAUD.......................................................................................................... 7
BEST PRACTICES ...................................................................................................................................... 10
CONCLUSION ................................................................................................................................................ 12
ABOUT AITE GROUP...................................................................................................................................... 13
AUTHOR INFORMATION ......................................................................................................................... 13
CONTACT................................................................................................................................................. 13

LIST OF FIGURES
FIGURE 1: INCREASING INVESTMENT IN CONTACT CENTER FRAUD TECHNOLOGY ................................................. 9

LIST OF TABLES
TABLE A: APPROACHES TO CONTACT CENTER SECURITY ........................................................................... 7
INTRODUCTION

“Be like water making its way through cracks. Do not be assertive, but adjust to the object, and you shall find a way around or through it.” –Bruce Lee

Following Bruce Lee’s advice, fraudsters have proven adept in their ability to study their target, identify weakness, and follow the path of least resistance. Increasingly, that path is leading criminals directly to financial institutions’ (FIs’) contact centers. Contact center fraud is on the rise, successfully compromising the weakest link in the chain—the human being.

The online channel has been the target of high-profile attacks for years, but as financial institutions bolster their online fraud mitigation capabilities, fraudsters are looking for softer targets. The contact center, with its customer service representatives (CSRs) who are trained and measured on their ability to provide high-quality, friendly customer service, represents easy pickings for the determined fraudster. Sometimes the fraud is solely perpetrated via the contact center, but more often it is just one target in a more complex cross-channel fraud scheme.

Financial institutions are responding, looking to technology to help with this point of exposure. Based on 20 interviews with fraud executives at North American financial institutions, this Aite Group white paper examines the ways in which criminals are successfully compromising the contact center and explores best practices in the FI response to this rising threat.
CONTACT CENTERS IN THE CROSSHAIRS

The attacks on contact centers emanate from many directions. International organized crime syndicates are responsible for the majority of the attacks, though opportunistic sole operators are also trying their hands with some degree of success. It is much easier to be a successful bad guy than a successful good guy; if the criminal is successful one in a hundred attempts, he or she will make off with a tidy sum. FIs, on the other hand, must seek perfection in their attempts to protect themselves and their customers.

Attacks on FIs are also growing increasingly sophisticated and complex. The distributed denial-of-service (DDoS) attacks against major U.S. FIs, which began in September 2012 and continued intermittently through the end of that year, were unprecedented in size and scale and brought the concept of cross-channel fraud to a whole new level. The DDoS attacks successfully brought down websites for some of the biggest financial brands, resulting in irritated customers and overwhelmed contact centers. The attacks were also publicized in advance; giving criminals notice that the FIs would be under attack and that their contact centers would be especially overwhelmed and vulnerable at that time. It is all too easy for a fraudster to take advantage of chaos to apply pressure to a frazzled contact center employee.

Fraudsters recognize not only that there are fewer layers of protection guarding the contact center than many of the other remote service channels but also that there is in many cases a human being whose emotions and weaknesses can be preyed upon. Contact centers are often the place where FIs route customers who require special treatment or exceptions—fraudsters understand this and capitalize on it as well. To that end, they’ve devised a wide variety of tactics to help them defeat the contact center’s rudimentary authentication measures and defraud the institution and its customers.

WAYS AND MEANS

Today, the majority of contact center authentication consists of little more than static challenge questions. Thanks to the ready availability of data on the Internet, these questions are often easily answered with a simple Web search or a visit to Facebook. In the event that the data is not available that way, criminals have found it only too easy to trick contact center reps into giving it up. The following are some of the common tactics that fraudsters are employing as they target contact centers.

- **Social engineering of phone reps:** CSRs are not trained to spot fraud, but rather to provide good service. Fraudsters understand this and will capitalize on the CSR’s desire to provide a positive customer experience.

- **Email and online chat takeover:** Contact centers are no longer limited to phone communications; often, communication with the customer comes in the form of email or online chat. Fraudsters are increasingly using email or chat credentials that have been compromised in one of myriad database breaches over the past couple of years to impersonate the customer and request transactions. While accepting email- or chat-based instructions is often against bank policy, the CSR is more focused on...
being responsive and keeping the customer happy than on the possibility that the request is fraudulent.

- **Sheer persistence:** Fraudsters will call the same FI over and over, and all too often FIs’ systems are able to detect neither that the calls are coming from the same individual nor whether the individual with whom the agent is speaking is the owner of the account. With each call, the fraudster gleans a bit more data until he or she gathers enough information about the targeted account and its owner to sail through authentication protocols and execute fraud. FIs have even seen fraudsters try to target specific CSRs who they find to be particularly vulnerable to social engineering. One FI shared that fraudsters figured out that the bank was monitoring call velocity on phone numbers and started using different phones to call in. The bank's fraud investigators tied the voices together by listening to the recorded calls, but the damage was done and the proceeds of the fraud long gone.

- **Take advantage of change:** System conversions as a result of bank mergers and acquisitions represent a great opportunity for fraudsters, who do their homework and recognize that the merging of two FIs is often inherently confusing for bank customers and contact center staff alike.

Once fraudsters have defeated the rudimentary authentication steps, they can lay the groundwork to cause financial loss in a number of ways:

- **Balance check or increase:** Often one of the first things bad guys will do is a simple balance check, which enables them to determine how much opportunity the account represents. Down the line, these bad guys will look to increase the balance available for fraud, for example via a request for a credit line increase.

- **Travel alert:** Requesting that a travel alert be placed on a cardholder's account enables a fraudster who has obtained compromised card data to create counterfeit cards and transact in geographic areas that are out of pattern for the actual cardholder.

- **PIN/password reset:** Many times the fraudster will request that the PIN on a debit card or the online banking password be reset. In these cases, the fraudster has already obtained either the card data or access to the individual’s account—likely thanks to the many database breaches over the past few years—and just needs to change the PIN or password.

- **Address, phone number, or email change:** The criminal will request that the contact information for the account be changed to lengthen the amount of time he or she has to perpetrate the fraud without the genuine account owner noticing the theft or in order to compromise out-of-band-authentication methods.

- **Order checks or a new debit or credit card:** The fraudster may order checks or a replacement card, often after having changed the address for delivery.

- **Wire request:** Wire transfers are one of fraudsters’ favorite mechanisms for moving money—fraudsters can get the biggest bang for their buck by requesting a wire be
sent to a new payee account. The money is gone instantly, and the loss amounts are usually sizeable. Consumer losses are maximized when funds are first transferred from credit lines, such as cards or equity lines, to a checking account, and they can easily run to six-figure amounts.

- **Bill-pay fraud**: The fraudster may add a new payee and make a large payment to an account he or she controls within or outside the financial institution. As with wire fraud, this method moves large amounts of money quickly.
MITIGATING CONTACT CENTER FRAUD

FIs are not standing idly by and allowing criminals to exploit this point of exposure. They are taking a number of steps in order to better protect the contact center. Similar to the online channel, many FIs are layering their approach to contact center fraud mitigation, using multiple complementary technologies at once. Indeed, in the United States, many FIs interpret the June 2011 Federal Financial Institutions Examination Council (FFIEC) Supplemental Guidance for Online Authentication as applying not only to the online channel but also as requiring a layered, risk-based approach to security in all remote channels. Table A provides an overview of a variety of ways in which FIs are securing their call centers.

Table A: Approaches to Contact Center Security

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
<th>Aite Group’s take</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANI</td>
<td>Automatic number identification (ANI) provides the receiver of a call with the number of the caller.</td>
<td>Moderately effective: ANI can be useful for catching amateur fraudsters. Of course, ANI alone doesn’t help much, but if ANI feeds into a velocity system that can flag a high velocity of inbound calls, or if ANIs associated with known fraudsters feed into an internal negative file, ANI data can be quite useful. ANIs are easy to spoof, however, so more sophisticated fraudsters have a relatively easy time bypassing the velocity and negative-file controls.</td>
</tr>
<tr>
<td>Audio analysis</td>
<td>Analysis of the call signal to determine type of device used to originate the call, network, and location.</td>
<td>Moderately effective: Audio analysis is a good tool, particularly when used in conjunction with behavioral analytics.</td>
</tr>
<tr>
<td>Static KBA</td>
<td>Static knowledge-based authentication (KBA) provides questions based on preset questions and answers established at the time of account opening.</td>
<td>Ineffective: Static KBA is quite ineffective, thanks to the prevalence of personal data on the Internet and the ease with which fraudsters can socially engineer call center reps to glean the answers.</td>
</tr>
<tr>
<td>Dynamic KBA</td>
<td>Dynamic KBA questions are generated on demand to perform customer authentication using databases that include data based on credit reports and/or demographic data.</td>
<td>Moderately effective: Dynamic KBA is more effective than its static counterpart, though credit-based questions can prove too difficult for the genuine consumer to answer; dynamic KBA is also often relatively expensive, so many FIs try to reserve for a limited set of use cases.</td>
</tr>
<tr>
<td>Behavioral analysis</td>
<td>Through rules and/or analytics, behavioral and interaction analysis tools detect fraud by identifying suspicious activities or patterns. Behavioral analysis in the call center examines not only the types of transactions engaged in but also the specific speech patterns and word usage to identify red flags associated with</td>
<td>Highly effective: Behavioral analysis technologies are well equipped to identify suspicious patterns of behavior that indicate fraud attempts. They can also be effective across multiple channels, identifying behavioral patterns that attempt to capitalize on the typical intelligence disconnects between products and channels. Interaction analysis technologies can also identify activities and speech patterns that are associated with fraud and tie these back to the fraudster’s call</td>
</tr>
</tbody>
</table>
Voice printing technologies create a unique identifier for the voice of the caller, then use that data on subsequent calls to identify the caller and determine whether a negative history is associated with the voice. Highly effective: Voice printing technologies have matured rapidly and are seeing positive results in FI implementations and pilots. The technology can reduce the number of false positives while highlighting suspect callers and flagging them for stepped-up authentication and/or holding transactions for further investigation.

Source: Aite Group

Technologies that are transparent to the end user, such as behavioral analytics and voice printing technologies, are preferred by FIs, which reserve the intrusion and cost of stepped-up authentication for only a small percentage of customers. Many FIs are looking to technology to help mitigate risk while maintaining high levels of customer care. Aite Group interviewed 20 senior fraud executives from large North American financial institutions to understand their planned use of advanced technology in the call center. When asked whether they plan to invest in voice technology as one method of protecting their call centers, 25% of FIs indicate that they either have a pilot underway or are working on a production rollout, while another 40% have voice technology on their one- to two-year call center roadmap (Figure 1).
Converging interests across the bank are all driving advanced contact center fraud mitigation capabilities. Retail bank product management executives are looking to the technology for higher levels of customer service and protection, while fraud and compliance groups are trying to address the rising fraud rates in the contact center and contact center operational management sees the technology's potential to prove operationally efficient.

Source: Aite Group interviews with 20 North American financial institutions, August 2012 to January 2013
BEST PRACTICES
As FIs deploy technology to address contact center fraud, they should adhere to the following best practices in order to maximize value:

- **Don't harm legitimate customers.** As with all fraud mitigation technology, the technology should take a risk-based approach and to the extent possible be transparent to the customer, reserving stepped-up authentication or more intrusive registration processes for higher-risk transactions.

- **Look across channels.** Fraudsters do not limit their attempts to any one channel, and neither should fraud solutions. This is particularly important in a contact center fraud solution, as so much of contact center fraud entails activity across multiple channels.

- **Leverage existing infrastructure.** It is much easier to champion a fraud solution business case if the solution can work within existing technology rather than require a wholesale infrastructure upgrade. FIs should look for a solution that can work seamlessly with existing call recording technology. Many FIs employ selective call recording for many of their call center processes; for the fraud mitigation technology to reach its maximum potential, it will optimally be able to analyze all call activity.

- **Employ collective intelligence.** Fraud is not a competitive issue but rather an industry-wide problem. The same fraudsters target multiple institutions, and FIs should look for a solution that can incorporate a consortium-data component. Shared negative files can help bring the combined knowledge and experience of the collective to bear.

- **Ensure the system can be tuned.** Each institution will have its own unique risk tolerances and fraud patterns. The solution should have tuning capability that allows the FI to dictate what constitutes a high-risk transaction and to even configure the key words and transactional sequences that are indicative of fraud.

- **Determine whether you need real-time or near-real-time capabilities.** While the trend is to try to take as many fraud mitigation capabilities to real time as possible, there is often a significant incremental cost associated with doing this in the call center. It is a much more expensive proposition to implement a fraud solution that can act on live voice calls than it is to leverage the call-recording technology already in place. For the majority of use cases, near-real-time capabilities are sufficient—the alerts can be generated and worked by analysts in time to prevent monetary loss.

- **Don't stop fraud management at alert creation.** Effective fraud mitigation technologies should incorporate the ability to create alerts as well as the ability to review, investigate, and manage fraud cases. Ideally, the system should be able to integrate with other transactional fraud detection systems.
NICE CONTACT CENTER FRAUD PREVENTION

NICE Contact Center Fraud Prevention monitors all contact center interactions for fraud, including screening against a watch list of known fraudsters. The solution provides a multi-layered fraud platform that combines voice biometrics, speech analytics, and context and telephony analytics to create a multi-factored interaction risk score. Low-risk interactions are automatically approved, whereas high-risk interactions can easily be further investigated via the NICE Actimize Risk Case Manager. NICE Contact Center Fraud Prevention is built with industry best practices in mind to maximize fraud detection capabilities while minimizing impact on customers and agents. The solution:

- **Doesn't harm legitimate customers**—reduces service hurdles by scrutinizing only high-risk interactions, while legitimate interactions go through without any interference

- **Takes a multi-layered, cross-channel approach**—increases detection with the NICE Fraud Platform using voice biometrics, speech analytics, and context analytics while integrating with Actimize's transactional systems for complete cross-channel protection

- **Leverages existing recording**—leverages your existing recording footprint to enable screening of all contact center interactions in a secure and scalable environment

- **Provides a scalable fraud platform**—brings together multiple technologies within one platform using a single user interface, including the ability to add new technologies down the line

- **Offers a consortium database**—broadens your fraud prevention capabilities by tapping into NICE's peer-to-peer network of key fraudster credentials

- **Provides real-time and near-real-time options**—strengthens deterrence by including real-time detection and NICE Real-Time Guidance to help agents appropriately handle high-risk interactions

- **Manages fraud from end to end**—minimizes losses by managing the full life cycle of high-risk incidents with NICE Actimize Risk Case Manager

These unique capabilities enable the enterprise to cut fraud losses without compromising customer experience and to cut operational costs by focusing fraud resources only on high-risk interactions.
CONCLUSION

Like water seeping through the cracks, criminals will continue to find new ways to defraud financial institutions and their customers. The contact center is one of the bad guys' new favorite targets, thanks to the susceptibility of human CSRs to social engineering and contact centers' lack of layered protection relative to other channels. Here are few recommendations for FIs looking to bolster their defenses:

- **Don't put all your eggs in one basket.** Fraudsters have proven adept at circumventing any single point solution. Just as the best practice for fraud mitigation in the online channel entails layered, complementary solutions, so should it in the contact center.

- **Create holistic defenses.** The attacks on the contact center are often just one part of a more complex scheme to defraud the institution, often including the online channel and one or more banking services. The solution set needs to take a holistic view of customer activity across products and channels.

- **Share ideas and experiential data with other FIs.** Fraud is not a competitive issue, and FIs can benefit from the experience of their peers. Look for solutions that enable collaboration and shared knowledge.

- **Don't be the last to deploy additional defenses.** The bad guys do their homework, performing reconnaissance and studying institutions to determine the best way to defraud them. If your FI is among the last to deploy robust contact center defenses, the bad guys will be sure to discover that and will concentrate their energies on FIs that represent low-hanging fruit.
ABOUT AITE GROUP

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

AUTHOR INFORMATION

Shirley Inscoe  
+1.704.987.5087  
sinscoe@aitegroup.com

Julie Conroy  
+1.517.992.5087  
jconroy@aitegroup.com

CONTACT

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

Aite Group Sales  
+1.617.338.6050  
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR  
+1.617.338.6050  
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com