Aite PARTNER. ADVISOR. CATALYST.

Combating Fraud:
Voice Biometrics in Contact Centers

© 2014 Aite Research and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

EXECUTIVE SUMMARY

Combating Fraud: Voice Biometrics in Contact Centers, commissioned by Verint and produced by Aite Group, addresses fraud occurring in financial institutions' contact centers and identifies how the use of voice biometrics can thwart this type of fraud.

Key takeaways from the study include the following:

- Seventy-four percent of financial institutions (FIs) state that organized attacks by criminal rings are responsible for the majority of their contact center fraud. As FIs strengthen their online controls, fraudsters are increasingly attacking contact centers as the channel of least resistance.
- Seventy-nine percent of executives report that account takeover and social engineering represent the majority of their contact center fraud. If fraudsters obtain customer credentials through social engineering, they may use them to commit fraud through other delivery channels, such as online.
- A large majority of fraudulent calls coming into financial institutions' contact centers are made by professional fraudsters, calling repetitively.
- Knowledge-based authentication (KBA) continues to lose favor with financial institutions as a method of mitigating fraud. Several executives report that their legitimate customers sometimes cannot answer dynamic KBA questions, while fraudsters have all the answers (for example, from a copy of the consumer's credit bureau report). For static KBA, fraudsters may make repetitive social engineering calls until they obtain the correct answers.
- Voice solutions have the potential to add value to financial institutions on several fronts: increasing operational efficiency, improving the customer experience via frictionless authentication, and reducing fraud losses.
- Voice biometrics can be used to successfully combat fraud, particularly with a negative file of fraudsters' voiceprints. After a fraud incident occurs, the recording of the call that led to the fraud is used to create the voiceprint; future incoming calls are then screened against the negative file, thwarting additional fraud attempts.
- Combining predictive analytics with voice biometrics adds value by improving the accuracy of matches and reducing false positives for fraud prevention purposes.

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

INTRODUCTION

Contact center fraud is growing in many financial institutions and will continue to grow as a favored method of attack unless FIs strengthen controls to make fraud far more difficult to perpetrate via this channel. According to Aite Group research, 53% percent of institutions that track losses related to contact centers report that losses are trending upward and that organized crime rings are most often the perpetrators. Given the sophistication of these criminal rings, current fraud-prevention methods in contact centers will prove increasingly inadequate over time. So long as fraud rings achieve more and more success in attacking this delivery channel, such attacks will grow as a favored mechanism to gain the data needed to take over the accounts of unwary victims.

Those intent on committing fraud are targeting the contact center more than ever before for several reasons. Many banks have made good progress in implementing the Federal Financial Institutions Examination Council (FFIEC) Supplemental Guidance for Online Authentication issued in 2011, which require that institutions have layers of security in the online channel. These guidelines have increasingly been applied to all remote delivery channels, although the online channel has received most of the attention. The result of FFIEC compliance has been a more secure online channel, causing fraudsters to look for easier access to the data they require in order to commit fraud. Continuing data breaches and hacking attacks supply much of the data needed to take over accounts; further, via social engineering, fraudsters are often able to intimidate, sweet-talk, or otherwise convince customer-service-focused contact center representatives into providing the final data elements required to gain online access or to order a new card or checks. While the types of fraud committed vary, the goal is the same: obtaining the required data or access vehicle to take over an account and steal money.

The recent distributed denial-of-service (DDoS) attacks that have targeted many large financial institutions and crippled their servers provide unprecedented opportunities for fraudsters. When the online channel is unavailable, contact centers tend to be inundated with unusually high call volume. For the sake of customer service, many representatives may be more lenient at this time and may not follow policies and procedures as carefully as they normally would. DDoS attacks are often publicized in advance, notifying organized criminal rings of when contact centers will be at their most vulnerable—when representatives are completely overworked and overwhelmed.

Voice biometric products are attractive to FIs as a mechanism to protect against these attacks; using a hot file of known fraudsters' voiceprints enables quick identification of a bad guy on an incoming call. In addition to fraud prevention, voiceprints have the potential to streamline the authentication process, thereby improving operational efficiency, and can increase customer satisfaction with the contact center experience.

METHODOLOGY

To understand the current trends of contact center fraud and the strategies that financial institutions are employing to combat it, Aite Group conducted 28 interviews with executives at 19 of the 40 largest financial institutions in the United States during Q1 2013. Executives

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

interviewed include those in charge of enterprise fraud management and enterprise loss prevention, regional and enterprise contact centers, and enterprise authentication strategists. Interviews covered the 40 largest financial institutions by asset size as follows:

- Five of the top 10 U.S. financial institutions
- Four of the top 11 to 20 U.S. FIs
- Four of the top 21 to 30 U.S. FIs
- Six of the top 31 to 40 U.S. FIs

Given the size of the research sample, the data provide a good directional indication of conditions in the market.

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

CONTACT CENTERS UNDER ATTACK

Many types of fraud are currently being committed via financial institution contact centers. Armed with information about a customer or accounts at the institution, fraudsters often engage in social engineering, making a series of calls to obtain additional information that fills gaps in the data they already have. Contact centers are often very large, so representatives are unlikely to answer more than one call from the same fraudster. After a series of social engineering calls, fraudsters often have adequate information to successfully impersonate the customer; at that point, they act to commit fraud. The unauthorized activity may result in setting up online banking for a customer who has never had it before, gaining access to an existing online relationship, ordering a new debit or credit card, initiating a wire transfer, or a wide variety of similar fraud scenarios.

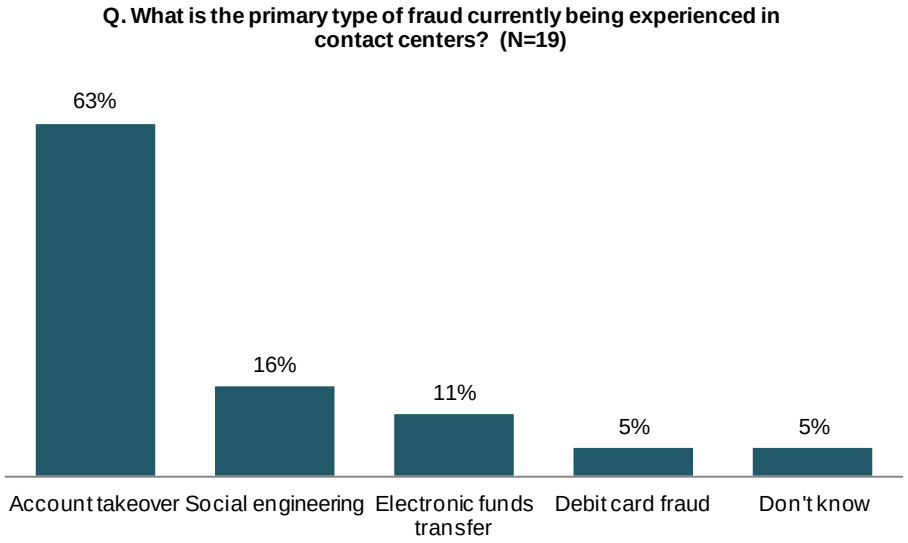
TRENDS IN CONTACT CENTER FRAUD

Interviewed executives state that the most prevalent types of fraud are social engineering and account takeover (of course, the first activity often enables the second). While the account takeover may be direct (by ordering a new card or checks, for example) several executives note that the contact center is often used to obtain the true customer's banking credentials, which are then used to commit fraud through other delivery channels—particularly through online banking. While these issues are similar for retail and commercial customers, most bankers agree that incidents with commercial clients occur less frequently but incur much larger losses when they do occur.

Sixty-three percent of executives name account takeover as the predominant type of fraud they are currently combating in their customer contact centers; an additional 16% feel that the primary problem is social engineering. Some types of fraud (electronic funds transfer and debit card) are also committed via account takeover but are named separately by executives whose fraud is heavily concentrated in those areas (Figure 1).

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

Figure 1: Leading Types of Fraud in Contact Centers



Source: Aite Group's interviews with executives at 19 of the top 40 U.S. financial institutions, January to March 2013

In order of significance, the table below ranks the types of fraud currently being experienced in contact centers. One institution does not monitor or examine contact center fraud and was unable to cite specific trends. Eleven percent of executives note that fraud targeting debit cards ranks as the most prevalent type of fraud experienced, while another 11% experience more electronic funds transfer fraud. As a secondary issue, 11% of executives note that a major reason for fraud losses is representatives who (knowingly or without understanding) violate policies or procedures that would have prevented the loss had they been followed. Another executive described how fraudsters are moving money into accounts operated by money mules, and the leaders of organized rings subsequently call to validate the amounts of the deposits; these fraud rings are truly being operated as businesses, with controls built in to detect missing funds from the accounts (Table A).

Table A: Rank Order of Primary Types of Contact Center Fraud

Financial institution	Highest-ranked fraud type	Secondary fraud type	Third fraud type
A	Account takeover	Policy violations	
B	Account takeover	New account fraud	
C	Account takeover	New account fraud	
D	Account takeover	Social engineering	
E	Account takeover	Policy violations	
F	Account takeover	Social engineering	New account fraud
G	Electronic funds transfer	Internal transfers	Unauthorized bill payments

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

Financial institution	Highest-ranked fraud type	Secondary fraud type	Third fraud type
H	Account takeover		
I	Account takeover	Social engineering	
J	Electronic funds transfer	New account fraud	Account takeover
K	Social engineering	Credit card fraud	
L	Debit card fraud	Social engineering	
M	Account takeover		
N	Don''t know		
O	Account takeover	Social engineering	New account fraud
P	Debit card fraud		
Q	Social engineering	Account takeover	
R	Account takeover	Social engineering	Electronic funds transfer
S	Account takeover	Social engineering	New account fraud

Source: Aite Group's interviews with executives at 19 of the top 40 U.S. financial institutions, January to March 2013

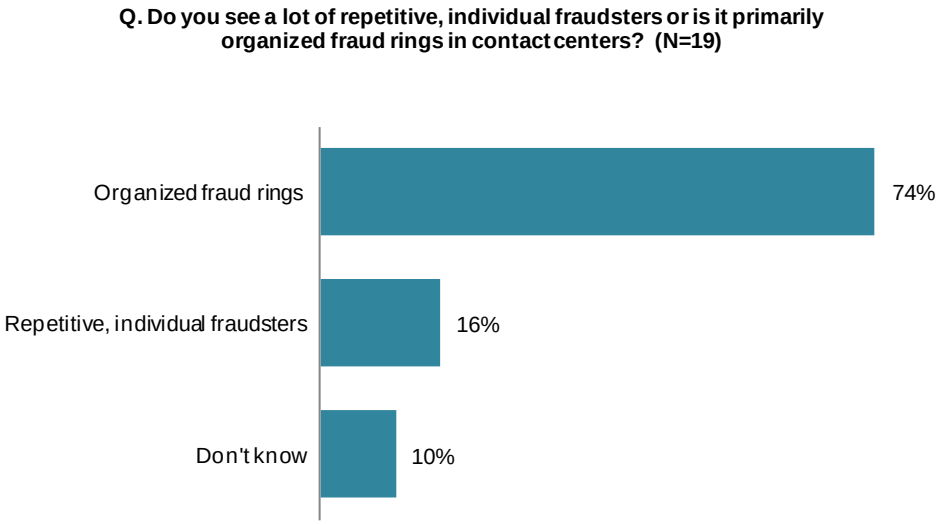
WHO ARE THE FRAUDSTERS?

Financial institution executives describe various attacks, from individuals who commit isolated fraud, to individuals who commit huge amounts of fraud by impersonating many different people, to organized fraud ring activity ranging from a few involved individuals up to dozens of people. Several recounted recent attacks that have been unusually focused for their institutions and led them to realize that the contact center requires more effective loss-prevention capabilities. In one example of this, a recent fraud ring obtained information about customers who had recently been in the hospital. The ring had data not only about these individuals (including their names, addresses, telephone numbers, and Social Security numbers) but also related to how these individuals paid their hospital bills. It is easy to understand how easily this ring was able to impersonate the institution's actual customers via telephone, given the amount of information already in its possession.

Three-quarters of FIs attribute the bulk of fraud to organized rings, while 16% have a greater problem with individuals who call repetitively. Indeed, as FIs are targeted by these organized fraud rings, executives estimate that as many as 80% to 90% of the fraud calls are originated by the same fraudsters calling over and over again. This is one primary reason the use of a hot file of fraudsters' voiceprints is so successful at detecting and identifying these fraudulent callers. Executives who have implemented voice biometrics state that once the fraudsters realize the FI is successfully recognizing their voice, they stop trying to perpetrate fraud against the institution. Ten percent of FIs don't have adequate information to know who is originating the attacks against them (Figure 2).

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

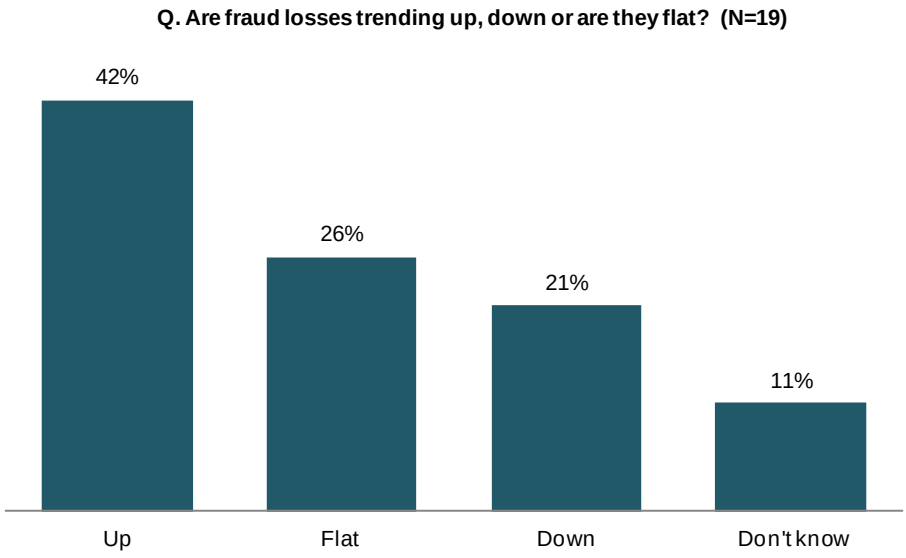
Figure 2: Fraudsters Attacking Contact Centers



Source: Aite Group's interviews with executives at 19 of the top 40 U.S. financial institutions, January to March 2013

In order to understand fraud loss trends, Aite Group spoke with executives about whether their contact center fraud losses are trending up, trending down, or staying flat. Forty-two percent confidently state that losses are definitely up, and some related this trend to recent fraud ring activity. A similar number responded, with varying degrees of confidence, that losses are flat or down. Executives at 11% of institutions say they really don't know the fraud loss trend due to poor tracking or lack of knowledge about the root cause of fraud losses (Figure 3).

Figure 3: Fraud Loss Trend in Contact Centers



Source: Aite Group's interviews with executives at 19 of the top 40 U.S. financial institutions, January to March 2013

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

EXISTING CONTACT CENTER SECURITY LAYERS

Financial institutions are not resting on their laurels while organized criminal rings take over their customers' accounts. Instead, they are fighting back, employing a number of technologies to try to protect customers. As stated previously, many are actively applying the FFIEC's Supplemental Guidance for Online Authentication to all remote channels, contact centers included; applying layers of security allows financial institutions to better protect their customers and themselves. Various technologies that can be used in contact centers are explained in Table B.

Table B: Approaches to Contact Center Fraud Prevention

Technology	Description	Aite Group's take
Automatic number identification (ANI)	ANI provides the receiver of a call with the number of the caller.	Moderately effective: ANI can be useful for catching amateur fraudsters if it 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. ANIs are easy to spoof, however, so more sophisticated fraudsters have a relatively easy time bypassing the velocity and negative-file controls.
Audio analysis	Analysis of the call signal to determine type of device used to originate the call, network, and location	Moderately effective: Audio analysis is a good tool, particularly when used in conjunction with behavioral analytics.
Static KBA	Static knowledge-based authentication (KBA) uses questions based on selected questions and answers established at the time of account opening (or updated thereafter).	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 contact center reps to glean the answers to registered questions. Changing static questions and answers periodically can make this more effective.
Dynamic KBA	Dynamic KBA questions are generated on demand to perform customer authentication using databases that include data based on credit reports and/or demographic data.	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 it for a limited set of use cases.
Behavioral analysis	Through rules and/or analytics, behavioral and interaction analysis tools detect fraud by identifying suspicious activities or patterns; behavioral analysis in the contact center examines not only the types of transactions engaged in—some technologies also can go a step further and analyze the specific speech	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 to further aid voice-printing technologies (defined below).

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

Technology	Description	Aite Group's take
	patterns and word usage to identify red flags associated with potential fraud.	
Voice biometrics	Voice-printing technologies create a unique identifier for the voice of the caller, then use that data on subsequent calls to positively 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

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

VOICE BIOMETRICS TO THE RESCUE

Voice biometric pilots are not new to the financial services industry; a number of institutions have piloted these programs during recent years. The technology has continued to improve, and FIs report that current solutions contain false positives at a fairly manageable level, particularly for passive voice recordings that create a hot file of fraudsters' voiceprints. In order to further reduce false positives and false negatives, some vendors add additional data elements to assess the risk associated with incoming calls. Such data elements may include Voice over IP (VoIP) anomalies, suspicious catchphrases, mispronunciation of the city the caller claims to live in, and other factors that raise suspicion about the caller's identity.

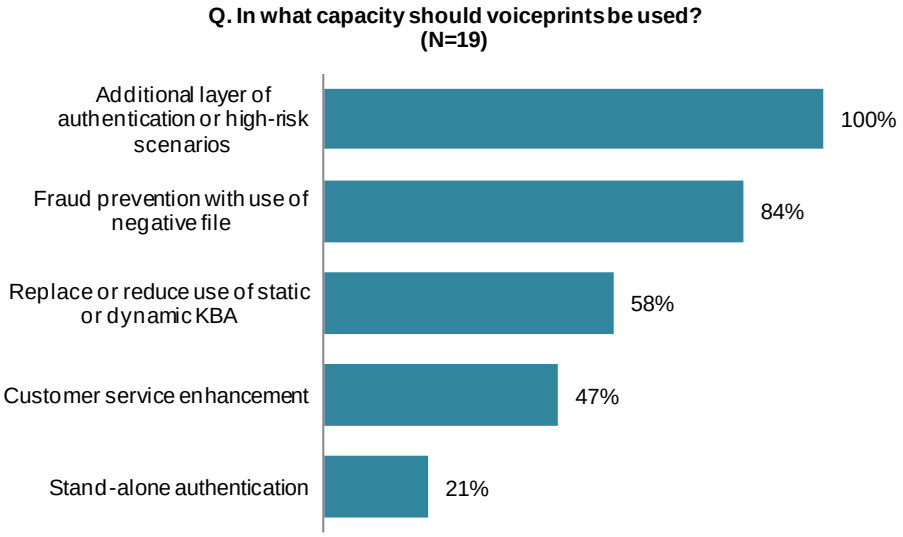
As FI executives weigh potential investment opportunities in contact centers, one that is rapidly gaining favor is voice biometrics. Voice biometrics offer not only a potential for fraud reduction but a potential method of customer authentication as well as cost savings via increased operational efficiencies. Operational efficiencies might be achieved in several ways: more effective use of the IVR to meet the needs of authenticated customers, more effective call routing (for example, sending a suspicious call to a group trained in dealing with potential fraud), and reducing or eliminating the use of knowledge-based authentication (KBA), a time-consuming solution that can alienate the legitimate customer. Financial executives' opinions may differ on which of these issues is of greatest importance, but most agree that the potential for all three benefits is well worth exploring. Voice biometrics may be the tool most needed to secure the telephone as a delivery channel.

POTENTIAL USE CASES

Voice biometrics is versatile in terms of accomplishing a number of things, and interviewed executives shared their views about various specific use cases. Every respondent executive agrees that voice products can be used as an additional layer in an FI's authentication strategy. Only 21% of executives believe that voice biometrics can be used as a stand-alone tool for authentication, however, as fraudsters have demonstrated over and over again their ability to overcome any single layer of security. In addition, the false positive and false negative rates could exclude voice biometrics as a legitimate authentication use case unless combined with other fraud-prevention capabilities such as behavioral or transactional analysis. The majority of executives also think that voice biometrics can be used to reduce losses (84% think so) and to eliminate or reduce the current use of KBA as part of customer authentication (58% think so). Forty-seven percent also see voice biometrics as a customer service enhancement that provides easier authentication and reduces friction in the customer interaction (Figure 4).

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

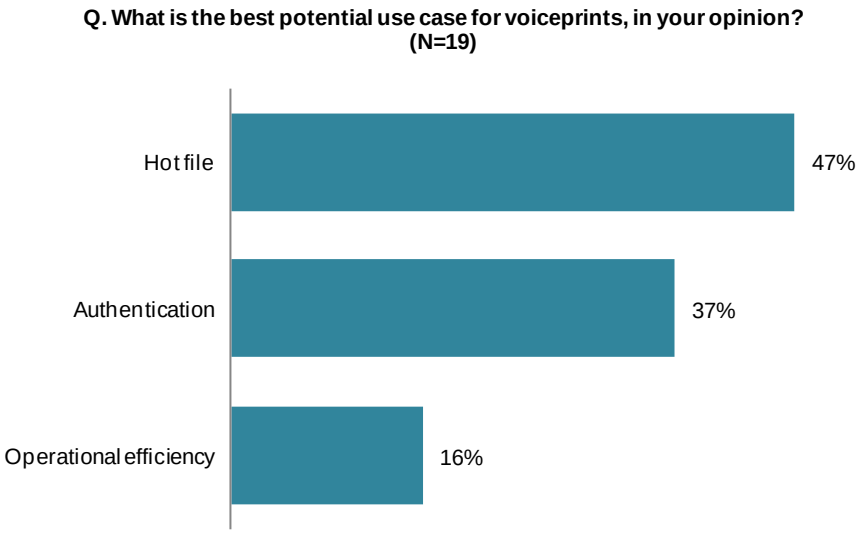
Figure 4: Legitimate Use Cases for Voice Biometrics



Source: Aite Group's interviews with executives at 19 of the top 40 U.S. financial institutions, January to March 2013

Further refining their opinions concerning voiceprint use cases, executives named what they see as the best potential use case for voice. Among respondent execs, 47% state that the best voiceprint use case is a negative file to reduce fraud losses; the majority sees this use case as the simplest one to achieve and plan to implement it prior to other use cases, even if they believe other use cases are of greater value. Thirty-seven percent see authentication as the most useful capability, while 16% most highly value the operational efficiency savings they expect to achieve (Figure 5).

Figure 5: Best Use Case for Voice Biometrics

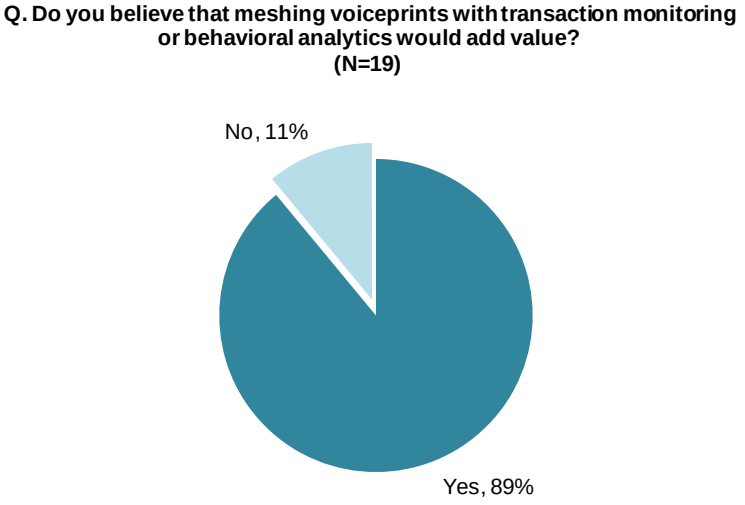


© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

Source: Aite Group's interviews with executives at 19 of the top 40 U.S. financial institutions, January to March 2013

While executives have high hopes for the fraud reduction that voice biometric solutions enable, 89% also believe that voice products can be a valuable additional layer of security, particularly when combined with other fraud prevention capabilities such as transaction monitoring or behavioral analytics. Each additional layer of security further reduces false positives and provides additional insight into the suspicious activity being reviewed. Factoring in additional elements such as ANI, call metadata, etc., also enables a risk score to be derived for each suspicious call and assists in keeping false positive rates low. As fraud executives know, scoring alerts helps determine which are the most critical, particularly when an institution is under attack. As one executive summarized, "There is no silver bullet. This [voice biometrics] would add a new data element to refine fraud-prevention efforts" (Figure 6).

Figure 6: Value as an Additional Security Layer



Source: Aite Group's interviews with executives at 19 of the top 40 U.S. financial institutions, January to March 2013

A BUSINESS CASE FOR VOICE SOLUTIONS

Seldom are new solutions introduced that have the potential to satisfy so many of financial institutions' different needs and desires. Management in several areas may be interested in learning about voice solutions: contact centers, the fraud prevention department, the mobile delivery channel and potentially other areas of the financial institution (e.g., wealth management). Having all these areas interested in a similar solution may help accelerate the purchasing process.

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

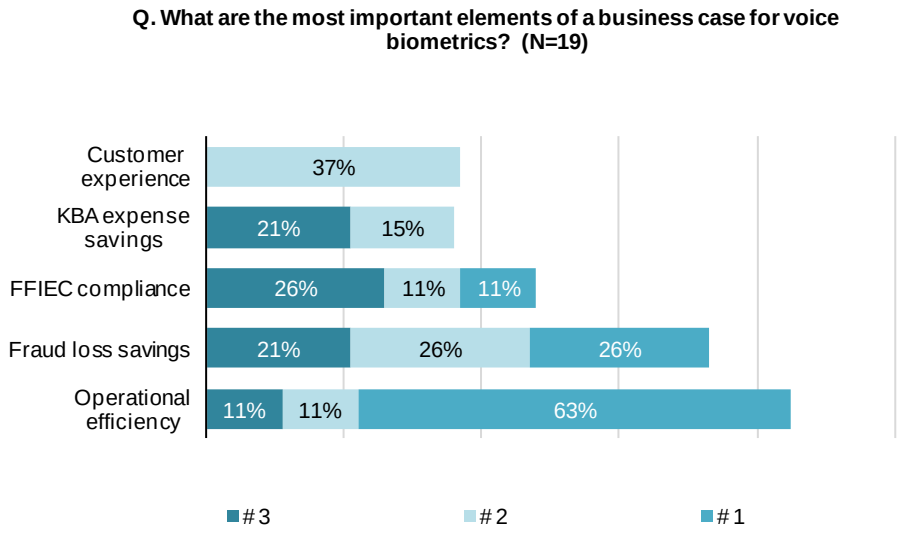
Before any new solution can be implemented at a financial institution, a business case must be created to justify the expense, and that business case must be approved and funded by executive management. Here is where the true beauty of the multiple benefits of voice solutions lies. As discussed previously, most executives want to achieve multiple benefits with a voice solution: operational efficiency savings, fraud loss reduction, and streamlined authentication leading to an improved customer experience.

Typically, seeking funding for any new solution involves fierce competition for scarce investment dollars. Fraud solutions don't always fare well in such a competition, particularly if the internal competition arises from business cases that will generate additional revenue or achieve required regulatory compliance. Given that multiple areas of an institution (fraud, authentication, contact center management, retail bank) will have goals tied to a business case for voice solutions, approval rates should be much improved. As fraud professionals know, having a sound business case does not always lead to success, and having the support of multiple business units is beneficial.

Interviewed executives prioritize the items most important to a sound business case for voice solutions somewhat differently, sometimes based on their roles. Those who understand the cost structure of the contact center (63%) tend to state that operational efficiency is the most important element in the business case. Institutions that have experienced the highest fraud losses (26%) believe that reducing those is most important. Eleven percent of executives feel that playing up the compliance angle—the FFIEC requiring layers of security for remote channels—would be most beneficial to gaining approval.

As a secondary measure of success, 37% of executives maintain that the management teams at their institutions emphasize improving customer satisfaction; these execs point out that simplifying authentication would lead to faster service and less friction in that process (Figure 7).

Figure 7: Key Business Case Elements



Source: Aite Group's interviews with executives at 19 of the top 40 U.S. financial institutions, January to March 2013

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

ABOUT VERINT AND VICTRIO FRAUD DETECTION FOR CONTACT CENTERS

Fraud detection from Victrio (now part of Verint Systems) is an anti-fraud technology for contact centers that uses voice biometrics and predictive analytics to detect attacks and deter fraudsters. This Verint Fraud Detection solution screens calls against a database of known fraudsters and alerts voiceprint matches to the organization. The solution works in the background of a call, without caller interruption, and can operate in real-time or near-real-time.

Verint Fraud Detection augments voice biometric scoring with predictive analytics on other passive factors, including call, account, and other metadata. With this multifactor scoring process, Verint Fraud Detection achieves high accuracy at scale, meeting high detection and low false positive rates even while screening millions of calls against large fraudster databases in the thousands.

Verint Fraud Detection is deployed at major banks and card issuers in some of the industry's largest implementations of voice biometrics for fraud detection. Verint's years of experience in combining voice biometrics, fraud analysis, and contact center operations provide expertise in successful fraud detection at a large scale.

The Verint Fraud Detection system provides:

- **Voice biometric screening of calls for fraudster matches**, achieving accuracy at scale for large fraudster databases and call volumes
- **Discovery and the addition of new voiceprints** to the fraudster voiceprint database
- **Predictive analytics to spot suspicious patterns and trends** across other passive factors, like call, account, and other metadata
- **Compelling results**, including reduction in fraud attacks, deterrence of fraudsters over time, and savings in fraud losses
- **Managed service** to provide system performance tuning and continued insights into changing fraudster behavior
- **Integration with existing call center recording infrastructure**, readily leveraging existing call recordings and operational process

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

CONCLUSION

In combating contact center fraud, financial institution executives should:

- **Be informed:** Monitor progress on all forms of biometrics as well as consumer reaction and legislative developments.
- **Network with internal departments:** Coordinate internal efforts and gauge interest in voice biometrics from other departments that may benefit from it; enlist support when preparing and presenting a business case to executive management.
- **Network with peers externally:** Ensure you monitor industry progress and are knowledgeable concerning fraud-prevention efforts at other institutions so your FI doesn't fall behind on fraud-prevention efforts and become a primary target of organized fraud rings.
- **Accurately track fraud losses:** Consider refining analysis of losses originating from activity in contact centers so it will be accurate for use in a potential business case. While contact center losses may not currently be a priority, they may rise quickly if competitors implement solutions to address them.
- **Be proactive:** Enlist the support of industry associations to assist with educating consumers and legislators. Enlist industry associations and lobbyists, as appropriate, to influence new legislation.

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

ABOUT VERINT

Verint® (NASDAQ: VRNT) is a global leader in Actionable Intelligence® solutions. Actionable Intelligence is a necessity in a dynamic world of massive information growth because it empowers organizations with crucial insights and enables decision makers to anticipate, respond and take action. Verint Actionable Intelligence solutions help organizations address three important challenges: customer engagement optimization; security intelligence; and fraud, risk, and compliance. Today, more than 10,000 organizations in over 180 countries, including over 80 percent of the Fortune 100, use Verint solutions to improve enterprise performance and make the world a safer place. Learn more at www.verint.com.

In 2013, Verint acquired Victrio™, an innovator in fraud prevention and authentication solutions. The combination of Verint and Victrio advances this comprehensive solution set by combining industry-leading voice biometrics and predictive analytics with enterprise workforce optimization solutions, furthering the company's portfolio of fraud, risk and compliance solutions.

CONTACT

For more information, contact:

Verint Systems Inc.

1-800-4VERINT

+1-631-962-9600

info@verint.com

www.verint.com

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.

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
+1.617.398.5050
sinscoe@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
+44.(0)207.092.8137
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

© 2014 Aite Group and Verint Systems. All rights reserved. Reproduction of this white paper by any means is strictly prohibited.