Aite PARTNER. ADVISOR. CATALYST.

Digital Channel Fraud Mitigation: Evolving to Mobile-First

NOVEMBER 2017

Shirley Inscoe

This Aite Group report is provided compliments of:

Early Warning®

TABLE OF CONTENTS

LIST OF FIGURES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- This research was based on telephone interviews with 28 executives in 19 North American financial institutions (FIs), and it focuses on the online and mobile channels.
- Leading FIs are adopting a mobile-first strategy and are introducing new products and capabilities via the mobile channel first in the belief that mobile activity can be better secured and is even more attractive to customers than online access.
- Compared to two years ago, digital channel fraud losses are up at 74% of large North American FIs, despite all the technology investments made in recent years.
- Identity crimes (account takeover [ATO] and application fraud) are leading types of digital channel losses; other fraud loss types that are increasing include mobile remote deposit capture (mRDC), card-not-present (CNP) fraud, and first-party fraud.
- Phishing attacks, data breaches, and authentication gaps are leading pain points that fraud executives are grappling with.
- Seventy-nine percent of large FIs anticipate increased technology spending in the next one to two years for digital channel fraud mitigation.
- Due to factors such as data breaches and phishing attacks, some legacy forms of authentication are not as effective as they have been in the past; as a result, FIs will decrease reliance on high-friction methods such as knowledge-based authentication (KBA), hard tokens, and online credentials.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

Digital channels are very attractive to FIs because the online and mobile channels enable FIs to offer products and services much more cheaply than in a branch or contact center environment. Digital channels also enable consumers and businesses to bank with them regardless of geographic location. Unfortunately, it is increasingly difficult to determine the identity of the party on the other side of the computer or smart device due to all the data breaches, phishing attacks, and social engineering tactics as well as the growing malware threat.

This report is a refresh of research published by Aite Group in 2015[1] and is part one in a two-part series; the first report examines what the current fraud trends are in North American FIs' digital channels, how FIs currently protect them, and how they plan to protect them in the future. The second report will look at new trends affecting FIs' strategies to protect digital channels, such as the rise of authentication hubs, the growing importance of removing authentication friction to improve the customer experience, and how information security and fraud departments can collaborate to benefit the FI. The mobile and online channels are the future; authenticating returning customers and determining who new applicants really are will be essential to successfully expanding product offerings in a high-risk environment.

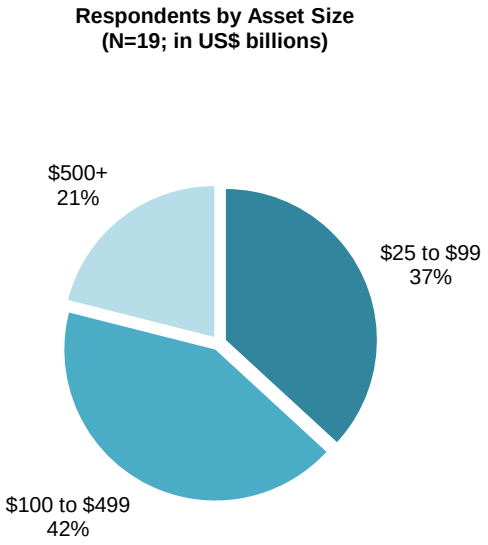
METHODOLOGY

To understand current trends in online and mobile banking fraud as well as the tools being used to mitigate fraud, Aite Group conducted telephone interviews with 28 fraud and digital channel executives from 19 North American FIs that have more than US$25 billion in assets from July to September 2017. Figure 1 shows the breakdown of participating FIs by asset size. Sixteen of the banks have U.S. operations, and the other three operate in both the U.S. and Canada.

1. See Aite Group's report *Digital Channel Fraud Mitigation: The Mobile Force Awakens*, June 2015.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 1: Asset Size of Participating FIs



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

THE MARKET

In 2015, many FIs were experiencing declining or flat fraud losses in their digital channels thanks to the many technology investments that they had made. Also, in 2015, criminals were primarily focused on wholesale banking, with targeted malware-based corporate ATO attacks. In 2017, those corporate ATO attacks continue, but the criminals' primary focus has shifted back to the retail channel. In today's market, fraud losses are rising at many FIs, particularly losses due to identity crimes. The recent large data breaches add more fuel to the fire of identity crimes and lead to higher fraud losses for FIs (Table A).

Table A: The Market

Market trends	Market implications
Fraud losses are rising among many large North American FIs.	Technology spend will increase at many FIs as they upgrade current solutions or invest in new ones to combat fraud.
Identity crimes, such as ATO and application fraud, are top concerns.	FIs will focus on using more transparent technologies to determine that the person is who he or she claims to be.
FIs are focused on improving the customer experience and removing friction from many current processes.	Business cases for fraud technologies are more likely to gain approval if they reduce friction; solutions that introduce more friction are less likely to gain approval.
FIs are offering many more products and services via the mobile channel.	As higher-risk activities are offered via mobile and as transaction volume grows, fraud rings will focus more on this channel. Some leading FIs are bringing new functionality to the mobile channel first due to the upsurge in mobile banking activity.

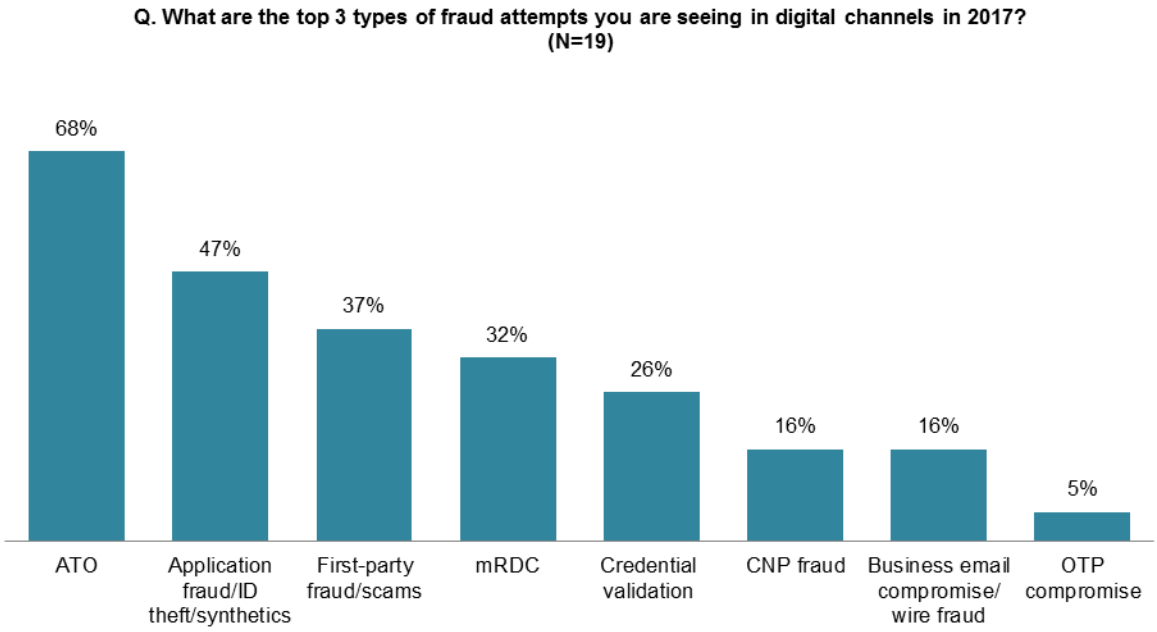
Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

THREAT ENVIRONMENT

The current threat environment is rife with fraud attempts in digital channels. New variations of fraud are seen commonly, so adjustments must be made quickly to counter new attacks. Identity crimes are especially prolific, and ATO and application fraud are the two most common attack types currently experienced in the market. Executives also bemoan how often their customers fall for a wide variety of scams, providing their credentials to fraudsters or clicking on a link that enables fraudsters to install malware that later harvests their credentials. Check fraud is back in vogue with fraudsters, and they are taking advantage of mRDC (along with other traditional channels, such as branch and ATM) to commit it. Bot attacks are increasingly being used to try credentials from data breaches on FI sites until the fraudsters find a site one which they work. CNP fraud is increasing in the wake of EMV rollout, but at a slower clip than estimated. Wire fraud and Automated Clearing House (ACH) fraud on commercial accounts continue unabated with email account compromise often being a root cause of the fraud. One FI respondent notes that his FI has been targeted with one-time-password (OTP) compromises (Figure 2).

Figure 2: Most Common Fraud Attempt Types in Large North American FIs



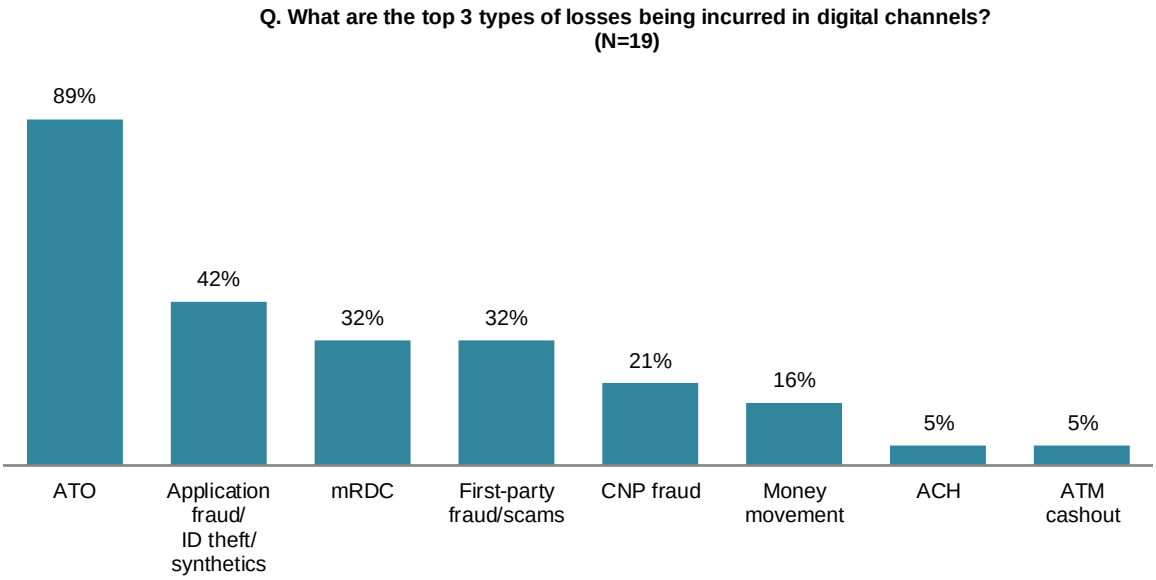
Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Of course, when fraudsters focus on certain types of fraud and continue their attempts, losses will inevitably result. No solution can detect or prevent 100% of fraud attempts. By far, the type of fraud losses currently leading in digital channels is ATO fraud, followed by application fraud. The growth in these identity crime losses demonstrates FIs' increasing difficulty with correctly and consistently determining who they are dealing with in the digital realm. Fraud losses are growing due to mRDC, first-party fraud, customers who fall for scams, and CNP fraud. In addition, current losses are higher in many FIs due to money movement or transfers,

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

unauthorized ACH payments, and ATM cashouts. Organized fraud rings have been using malware to attack ATMs[2] in other countries in recent years, and that activity is now being seen by North American FIs as well (Figure 3).

Figure 3: Most Common Fraud Loss Types in Large North American FIs



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

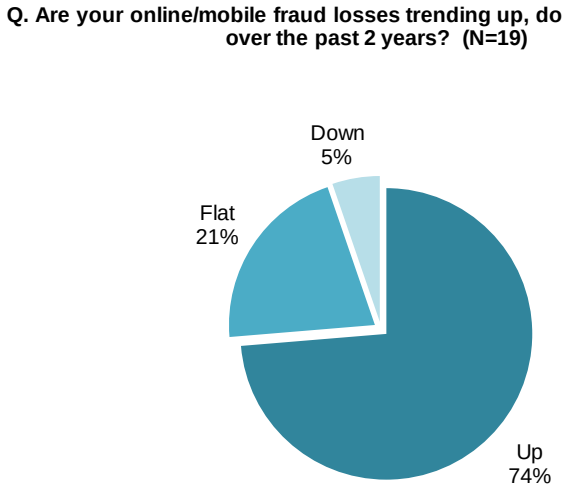
Digital channel fraud losses are on the rise at 74% of large North American FIs; losses are flat in 21% of FIs and down in only 5%, as shown in Figure 4. This is a considerable change from the environment in 2015, when losses were up in only 16% of FIs and down in 47%.[3]

2. See Aite Group's report *ATM Fraud: Increasingly Organized*, November 2016.

3. See Aite Group's report *Digital Channel Fraud Mitigation: The Mobile Force Awakens*, June 2015.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

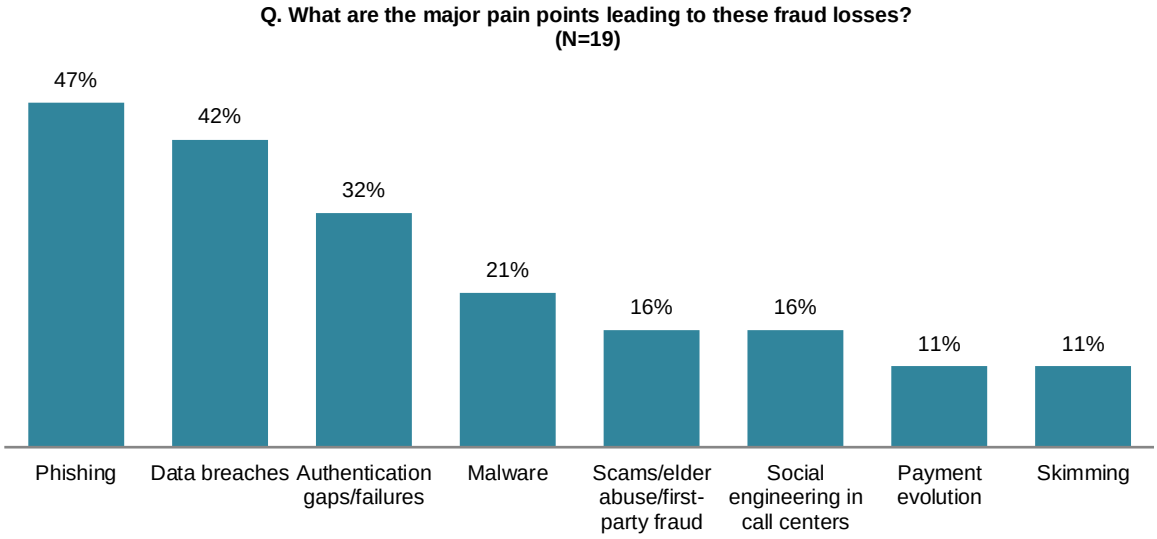
Figure 4: Trajectory of Online/Mobile Fraud Losses for Large North American FIs



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

FI executives name many pain points that are leading to this uptick in fraud. These pain points are generally beyond their control but enable fraud attacks or fuel a much higher volume of them. Figure 5 shows the pain points named most frequently by FI executives.

Figure 5: Commonly Named Pain Points Enabling Fraud



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

The most commonly named pain points are described as follows:

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- **Phishing**: Phishing occurs when a fraudster sends an email to a consumer purporting to be from a trusted source (a business or an individual). These scams have grown far more sophisticated over the years and can appear to be legitimate. For example, the grammatical and spelling errors that were common years ago have been corrected, and the communications often frighten people into clicking on a link in the email or taking another action that enables the fraudster to gain access to their online credentials. Examples include an email purportedly from the IRS about tax filing errors or from the local energy company saying the account is past due and the electricity will be cut off if they do not respond. There are many variations; some offer good news, such as awarding a gift card or lottery winnings. In addition to email, these attacks have spread to mobile devices via text messages (smishing) and phone calls (vishing). The Anti-Phishing Working Group, a global industry, law enforcement, and government coalition focused on unifying the global response to electronic crime, reports there were more phishing attacks in 2016 than in any year since they started tracking them in 2004.[4] Phishing attacks rose 65% in 2016 compared to 2015; the total number of phishing attacks in 2016 was 1,220,523.

- **Data breaches**: Data breaches have grown so common that they were no longer big news until the recent breach at Equifax, which affected the personally identifiable information (PII) of 143 million consumers.[5] While much of this data was probably breached in earlier events, FIs have experienced an uptick in identity crimes, such as application fraud and ATO in 2017.[6] This trend has struck larger FIs particularly hard, but the attacks are trickling down to midsize and smaller FIs as well.

- **Authentication gaps/failures**: When millions of consumers' PII is in the hands of fraudsters, it is increasingly difficult to devise reliable authentication processes that verify a person's identity. Some methods used to authenticate consumers are more reliable than others. In a later section of this report, information is shared related to current and planned authentication processes in FIs.

- **Malware**: Malware is certainly not a new threat, but the nature of malware has changed. It is no longer likely to be developed by teenagers to prove what they can do, but instead it may be backed by governments, hacktivists, or criminal groups to steal data, cause destruction, or collect ransom. Malware has become more aggressive and more of a threat than ever before. The number of unique new malware strains continues to increase rapidly in both the online and mobile channels globally (Figure 6).

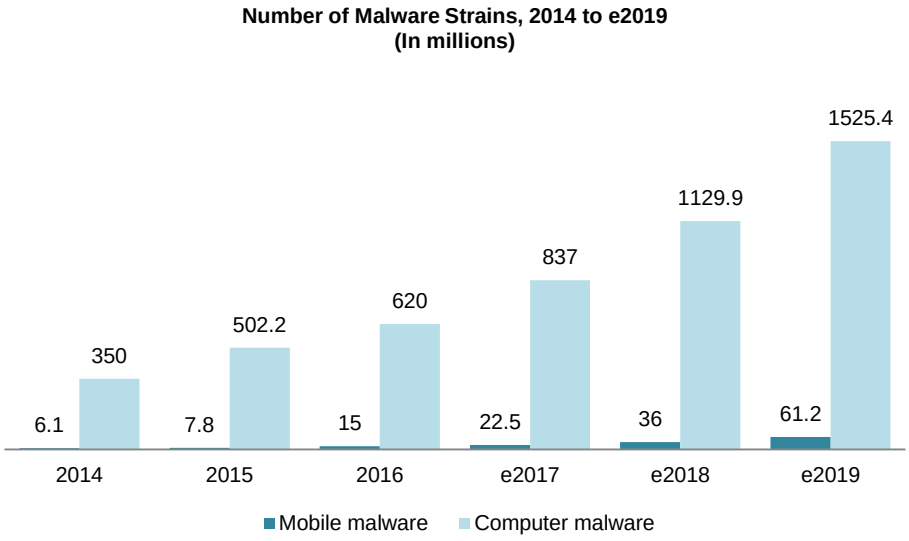
4. "Phishing Activity Trends Report, 4th Quarter 2016," Anti-Phishing Working Group, February 23, 2017, accessed September 19, 2017, http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf.

5. Lee Matthews, "Equifax Data Breach Impacts 143 Million Americans," Forbes, September 9, 2017, accessed September 20, 2017, https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#20117313356f.

6. See Aite Group's report *Financial Institution Fraud Trends: ATO and Application Fraud Rising Rapidly*, May 2017.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 6: Number of Unique Malware Strains



Source: McAfee, Aite Group

- **Scams/elder abuse/first-party fraud**: Fraud committed by your own customer is very difficult to detect and prevent. In addition, executives report that their customers are also falling for a variety of scams that lead to their accounts being compromised and money being stolen. It is common for fraudsters to target elderly consumers who may be particularly vulnerable to their scams. Traits such as loneliness, naiveté, and early stages of mental health issues may be factors in their susceptibility.

- **Social engineering in call centers**: Fraudsters often call repetitively until they are able to gather enough data to respond to KBA (aka out-of-wallet) questions and successfully impersonate a customer. Once the contact center agent accepts that the fraudster is the legitimate customer, the fraudster can take many actions, including resetting credentials for online or mobile banking, mailing a debit or credit card, or reordering check reorders. Contact centers, or the fraud enablement channel, are often the source of cross-channel fraud.[7]

- **Payment evolution**: Payments are increasingly mobile, and the U.S. is experiencing the advent of faster payments. While they may be able to adjust to faster payments, many FIs are just not ready for real-time payments. Fraud executives may not be ready, but many FIs are rolling out Zelle to their customers anyway; lacking a real-time interdiction capability may result in spiraling losses.

- **Skimming**: Although EMV cards have been issued by most FIs, magnetic stripes are still used widely because some merchants have not upgraded terminals and gas pumps were granted an extended deadline to upgrade, and fraud is widespread due

7. See Aite Group's report *Contact Centers: The Fraud Enablement Channel*, April 2016.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

to fallback transactions. Fallback transactions occur when the chip in an EMV card isn't read and the card is swiped instead. Counterfeit cards will continue to be used to commit fraud until magnetic stripes are discontinued, and skimming will continue as a major data source for counterfeit card creation.

In addition to the pain points listed above, several other pain points were each mentioned by only one executive; these pain points include an FI's fast growth rate, late rollout of EMV, a more lenient funds-availability policy for mRDC, and insufficient insight on customer behavior. Not surprisingly, one executive predicts that the industry's reliance on OTPs will become a pain point in the future.

PRIME TARGET: CONSUMERS

In recent years, businesses have been primary targets for fraud, most recently by business email compromises, in which a legitimate-looking email is apparently sent by an authority figure directing someone in the organization to originate a large funds transfer. This scheme has several variations and has been highly successful, leading the U.S. Federal Bureau of Investigations (FBI) to issue a public service announcement on May 4, 2017. In that announcement, the FBI stated that from October 2013 through December 2016, there were over 22,000 U.S. companies victimized, for potential losses of almost US$1.6 trillion.[8] These figures are especially troubling when one factors in the companies that may have lost funds but did not report falling for the scam to avoid negative publicity, or those that simply were not aware that they could report this activity. As a result, the number of events and amount of fraud losses are likely far higher than the public service announcement states.

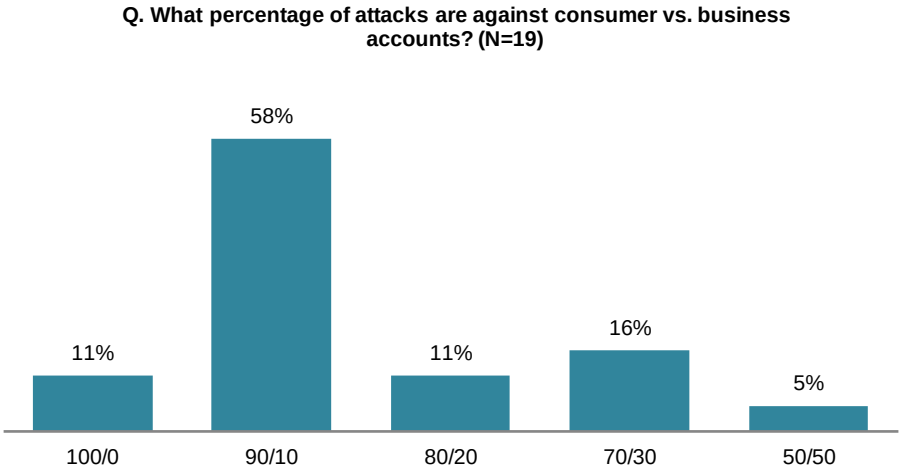
These attacks continue unabated, but the majority of attacks causing losses for FIs are directed toward consumer accounts. While business scams may result in far larger fraud losses per incident, the sheer volume of consumer fraud attacks and resulting losses overshadow these events.

Every FI has a unique customer base; some target consumers only, while others are primarily retail or business banks. Understanding that can help explain some of the different responses shown in Figure 7. For example, a bank that primarily has business clients is more likely to have higher rates of attacks against that portfolio. Largely, retail banks will have higher attack rates against retail accounts. Overall, the bulk of attacks are focused on consumer accounts. Only one FI reported even rates of attacks targeting consumer and business accounts; the majority (58%) report a 90/10 split.

8. "Business E-Mail Compromise, E-mail Account Compromise: The 5 Billion Dollar Scam," FBI, May 4, 2017, accessed September 27, 2017, https://www.ic3.gov/media/2017/170504.aspx.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 7: Consumer vs. Business Account Fraud Attack Comparison



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

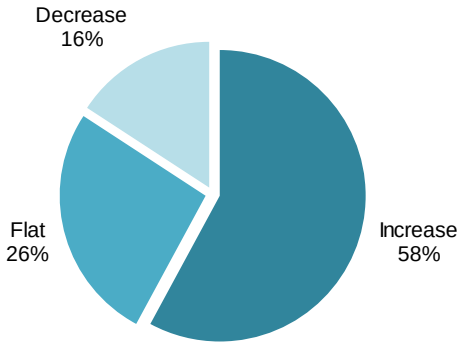
STAFFING BUDGET

Fraud executives have varying ideas related to their staffing budget in the next one to two years. Sixteen percent believe their staffing budget will decrease, largely due to plans to automate more of the work currently performed manually. Conversely, 58% state their staffing budget will increase due to new detection systems they plan to build internally or purchase. Several executives also comment that with faster payments on the horizon, they expect fraud alert volume to increase, necessitating additional staff. The remaining 26% believe their staffing needs will remain flat; they predict that increasing alert volume will be offset by planned automated process improvements (Figure 8).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 8: Future Staffing Budget Expectations

Q. Will your staffing budget remain flat, increase, or decrease in the next 12 to 24 months? (N=19)



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

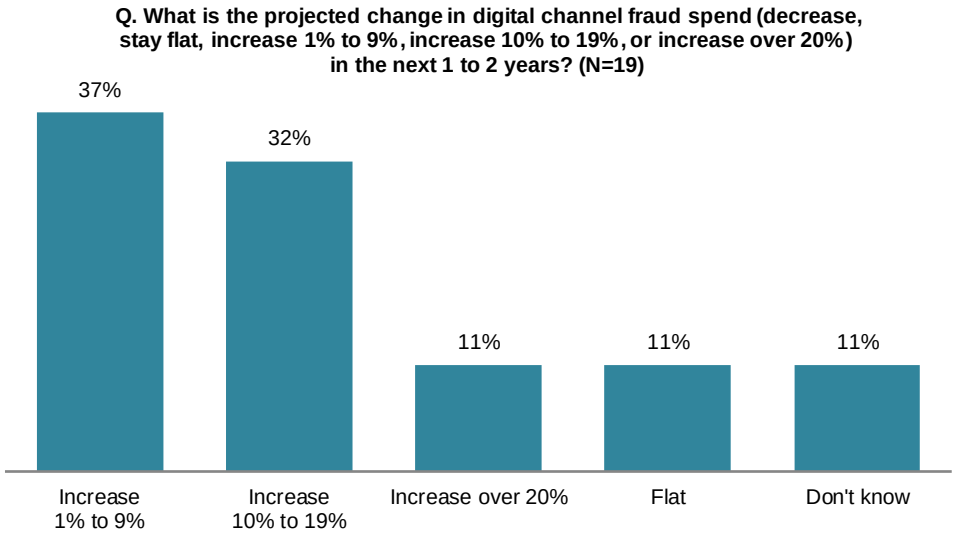
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CURRENT AND FUTURE USE OF DEFENSIVE TECHNIQUES

Gaining approval of a business case to improve fraud mitigation in digital channels is easier than it has been in recent years because fraud losses are growing and FIs want to offer more functionality via digital channels. Consumers are demanding more capabilities via their smartphones, and often these devices can help with authentication requirements to some degree. Certainly, it is an environment in which more customer self-service can be offered if the authentication process is strong and dependable. That represents a win-win because consumers can accomplish what they want quickly, and FIs can hold down costs. Some leading FIs are prioritizing new functionality in the mobile channel first, then developing it for the online channel, which is a reversal of the historic sequence of development.

The budget for digital channel investments will rise at the majority of FIs, with 80% stating they will increase spending at least slightly. Eleven percent of FIs state their technology budgets will rise more than 20%, and 32% state their budgets will rise 10% to 19% (Figure 9).

Figure 9: Anticipated Change in Digital-Channel Spend Among Large North American FIs

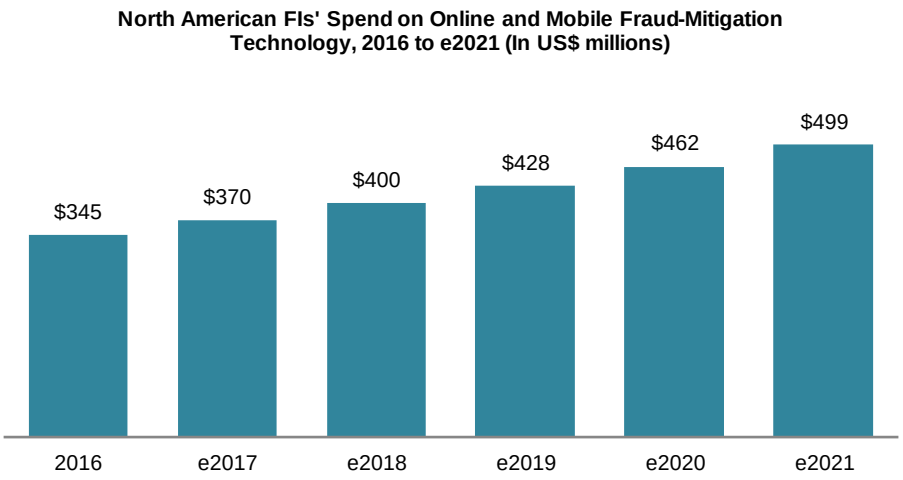


Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

In recent years, the amount of spend on protecting digital channels in North America has increased annually. As the mobile channel continues to improve in capabilities offered and grow in banking and payments activity, attacks against the channel will rival the rate of online attacks; therefore, the technology investment level will continue to grow. Mobile banking access rates already outnumber the rate of online access; these two channels will reverse in terms of significance and banking strategies focused on consumers in the next few years. By 2021, Aite Group estimates North American FIs will spend almost half a billion dollars annually protecting digital channels (Figure 10).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 10: North American FIs' Spending on Online and Mobile Fraud Mitigation

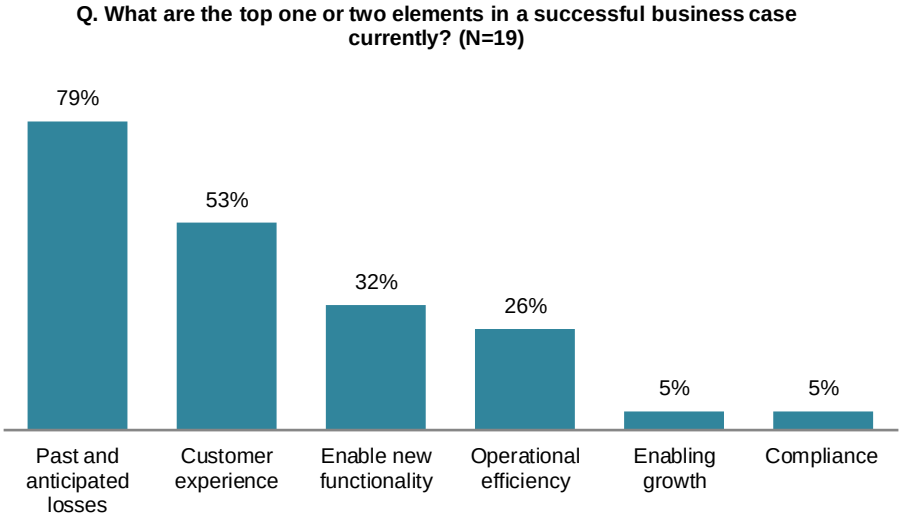


Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Before any new technology investment can be made by an FI, executive management must approve a business case. Many factors can help a business case win approval over all the other competing business cases, particularly those that increase FI profits. In today's environment, there is a big focus on the customer experience and trying to improve it, with specific emphasis on removing friction in various processes. FI executives note that the customer experience has a growing impact on whether a business case is approved. Several state that every business case is examined for its potential impact on the customer experience; however, the most critical element of a business case to better protect digital channels remains current and anticipated fraud losses. The second most important element in a business case is to improve the customer experience; the third most important element is to prepare for new functionality—notably, faster payments (Figure 11).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 11: Most Important Business Case Elements



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

PROTECTING DIGITAL CHANNELS

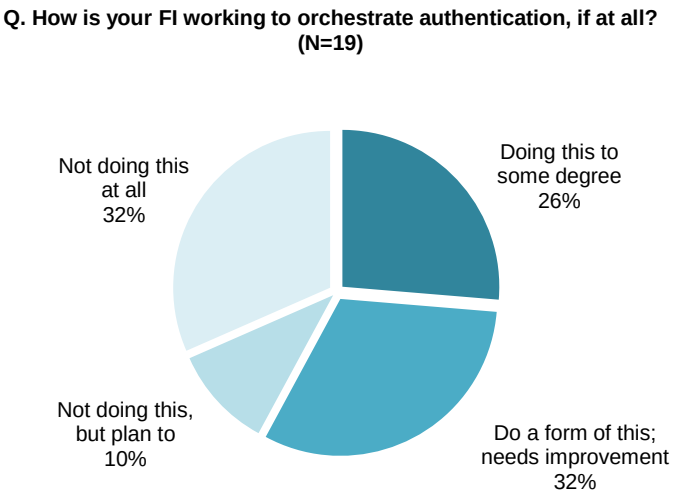
Knowing for certain who is on the other side of a device has become increasingly difficult, so FIs are not only reassessing the solutions they use to authenticate customers, but they are also changing their entire approach to authentication.

ORCHESTRATING AUTHENTICATION

Each FI has a unique strategy to authenticate customers and ensure applicants are who they claim to be; reliable authentication is the foundation of effective fraud prevention. As FIs employ a variety of solutions, they often use a waterfall approach with stepped-up authentication for high-risk transactions or a stepped-down approach for low-risk activities. Orchestration of authentication seeks to better analyze the customer's usual behavior patterns as well as the context of the transaction. It does away with the one-size-fits-all approach and instead only inserts the friction of stepped-up authentication when necessary, i.e., when the analytics flag that the context of the transaction is unusual. Effectively orchestrating authentication is desired by many, but in reality, it is in its infancy (Figure 12). There are many approaches to achieving this goal; they range from rudimentary to advanced analytics and sophisticated approaches that rely on machine learning.

Many executives report that they are overhauling their authentication strategies across all channels, looking for ways to strengthen them while minimizing customer friction. This is critical when PII is easily available to fraudsters, automated and organized attacks are increasing, and payments are rapidly evolving to become faster or real time.

Figure 12: Status of Orchestrating Authentication



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

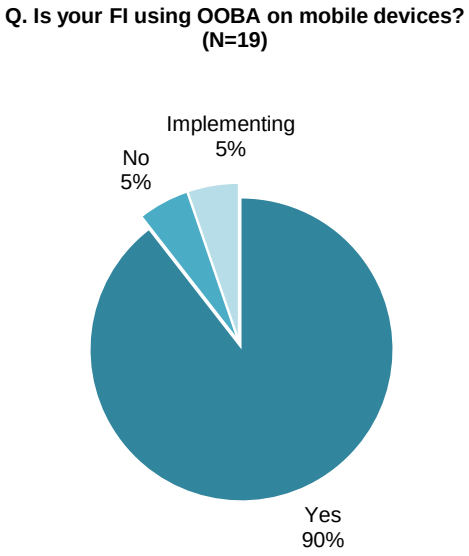
Solutions to protect digital channels include methods that have been in the market for decades as well as some that are relatively new and are only currently deployed by early adopters. This section looks at several methods used by FIs and how executives rate the effectiveness of each.

OUT-OF-BAND AUTHENTICATION (OOBA)

OOBA typically utilizes OTPs that can be sent to a consumer's computer or smartphone via voice message, SMS, email, or push notification. FIs that use OOBA sometimes offer more than one option to deliver the OTP, allowing the customers to choose their preference. However, not all methods of delivery carry the same level of risk. Other options some vendors incorporate in their offerings include transaction signing and voice biometrics to further authenticate the customer.

The use of OOBA has transitioned from a service that FIs ask customers to sign up for to one that is required for certain high-risk activities, e.g., wire originations or person-to-person payments. A large majority (90%) of FIs are using OOBA today (Figure 13).

Figure 13: FIs Using OOBA on Mobile Devices Currently



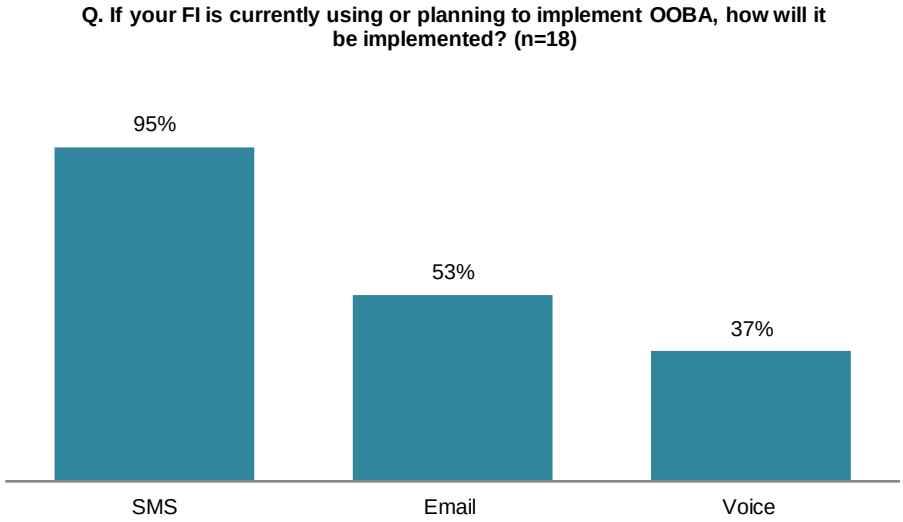
Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

As mentioned earlier, there are various ways OTPs can be delivered to the customer, and many FIs offer more than one option. However, the use of email to deliver OTPs is viewed somewhat as a necessary evil: One executive shares that fraud is 10 times higher when OTPs are delivered via email compared to SMS, and another bemoans the fact that his FI still offers email as a delivery option due to the higher risk. However, since some customers still don't use smartphones or do get charged for each text message, FIs may feel compelled to offer this option. SMS is clearly the most popular option, followed by email delivery and then voice (Figure 14).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

In 2016, the National Institute of Standards and Technology (NIST) published draft guidelines in which the use of SMS text was deprecated; it backed off this stance in its final guidelines, partially due to strong industry lobbying to allow the continued use of SMS texts.[9]

Figure 14: Methods FIs Use to Deliver OTPs



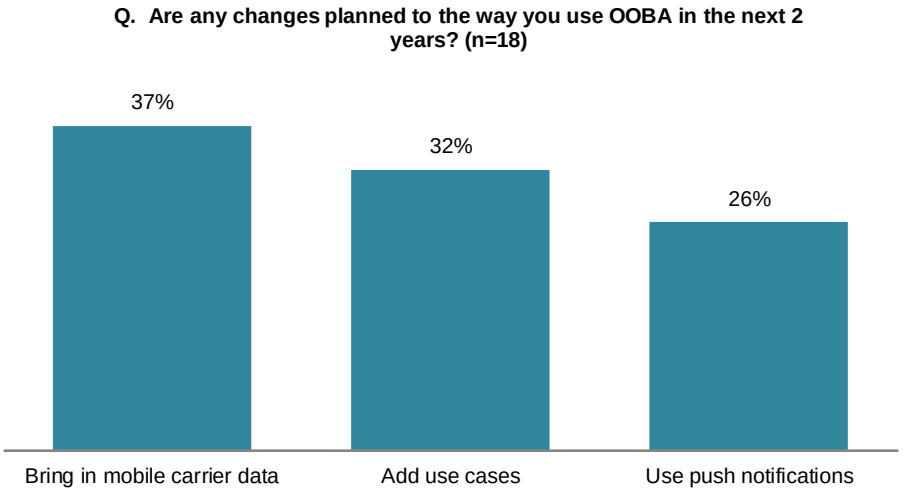
Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Figure 15 shows changes planned to the use of OOBA in the next two years. Due to the ready consumer acceptance of OTPs, one-third of FIs plan to increase the use cases for which they currently use OOBA; in addition, some FIs plan to offer push notification to improve security (in comparison to text and email) and overcome the challenge of consumers who get charged for each text message received. Several FIs that have not already done so plan to bring in mobile carrier data to help better secure SMS. This data can help protect against such threats as forwarded telephone numbers, SIM cards that have recently been swapped, or phones that have been jail broken.

9. See Aite Group's report *FFIEC and NIST Guidance: Mobile and Digital Requirements*, April 2017.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 15: Changes Planned for OOBA Use



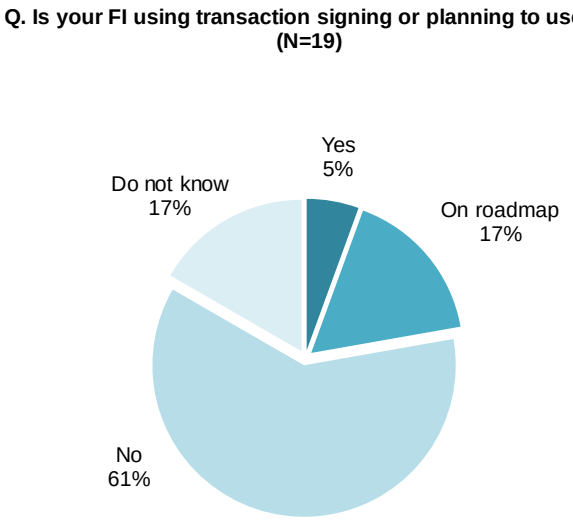
Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Another capability related to OOBA is transaction signing; this capability requires customers to digitally "sign" high-risk transactions.

Transaction signing is a relatively new capability, and some FI executives are still not familiar with it. It works by requiring the customer to input a dynamically generated PIN and is used to validate that none of the details of a transaction have been changed by malware or other threats. Transaction signing calculates a value based on the user input on both the client and server side; if the information doesn't match, the transaction will not be approved. An equal percentage of fraud executives are unfamiliar with transaction signing as those that have it on the roadmap to be implemented (17%). Only 5% are currently using transaction signing, and 61% have no plans to do so (Figure 16).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

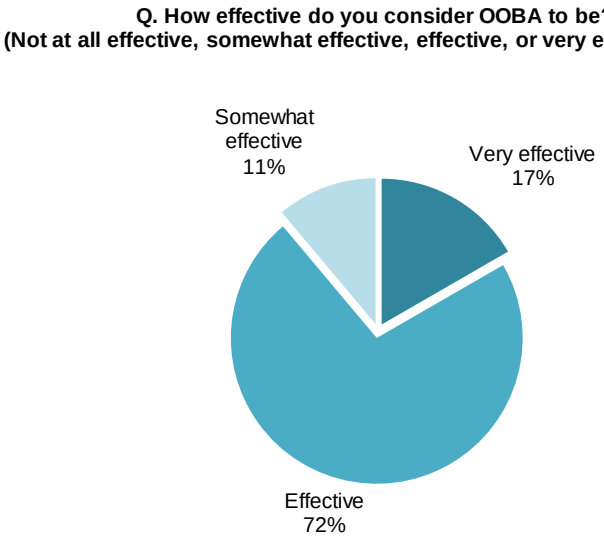
Figure 16: Use of Transaction Signing



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Overall, FI executives feel OOBA is effective, and a few consider it to be very effective. However, many note the need to shore up SMS with mobile carrier network data and note its limited effectiveness internationally. Eleven percent rate OOBA as only somewhat effective; two executives mention email as a weak delivery method, and a third executive rated OOBA as effective but then noted that it is only somewhat effective if email is used (Figure 17).

Figure 17: OOBA Effectiveness



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Many solution providers offer OOBA. Table B shows the leading providers in the market.

Table B: Leading OOBA Solution Providers

Solution provider	Headquarters
Early Warning Services	Scottsdale, Arizona
Encap Security	Fornebu, Norway
Entersekt	Cape Town, South Africa
Entrust Datacard	Minneapolis
Equifax	Atlanta
Gemalto	Amsterdam
HID Global	Austin, Texas
iovation	Portland, Oregon
Microsoft	Redmond, Washington
Oberthur Technologies	Paris
RSA Security	Bedford, Massachusetts
SecureKey	Ontario, Canada
Symantec	Mountain View, California
TeleSign	Marina del Rey, California
ThreatMetrix	San Jose, California
Trusona	Scottsdale, Arizona
TRUSTID	Lake Oswego, Oregon
ValidSoft	Tullamore, Ireland
Vasco	Oakbrook Terrace, Illinois

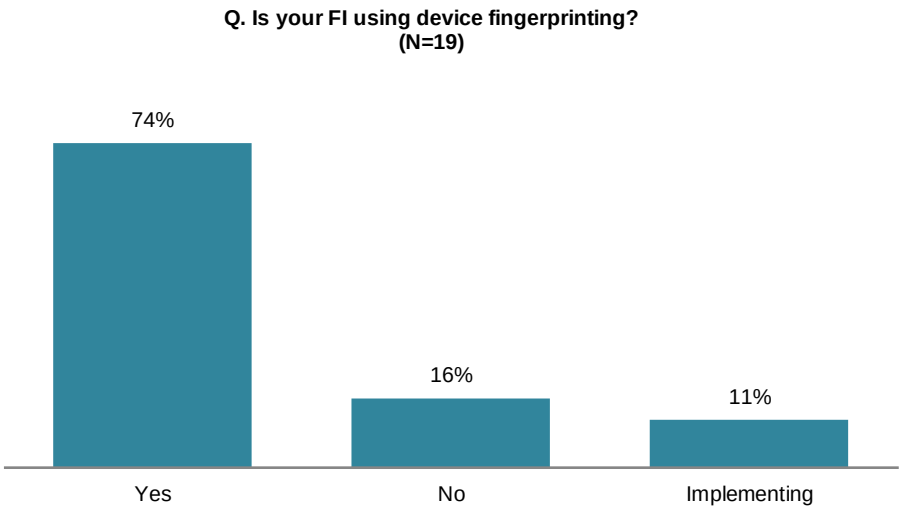
Source: Aite Group

DEVICE FINGERPRINTING

Device fingerprinting has come a long way in recent years; there are many features and capabilities of the mobile device that can be used to recognize it, and many FIs are starting to associate specific devices with particular customers. Knowing that a customer has used the device previously and that the transaction was not disputed can help as one layer in an effective authentication process. Of course, with smartphones, geolocation and many other factors can be used to perform analysis and detect suspicious activity. The majority of FIs (85%) are currently using or implementing device fingerprinting (Figure 18).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

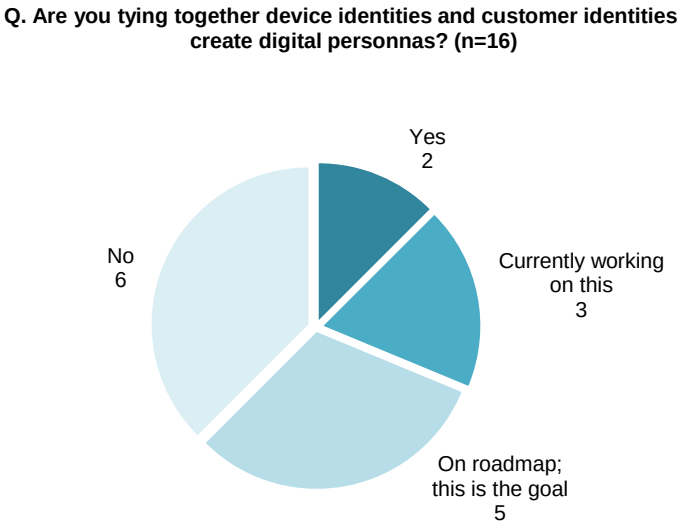
Figure 18: Use of Device Fingerprinting



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Many FIs plan to link the device fingerprint and the customer's identity to create digital personas. Doing so will enable them to more effectively authenticate their customer and reduce risk. This strategy is in very early stages of implementation, with only two large FIs having done quite a bit of work toward this goal. An additional three FIs are currently working toward doing this, and five more have digital personas on their 2018 roadmap (Figure 19).

Figure 19: Creation of Digital Personas

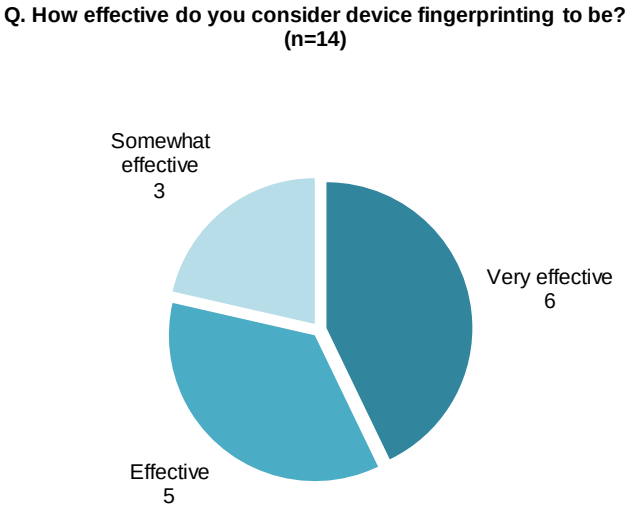


Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Overall, FI executives also consider device fingerprinting to be effective, with 11 of 14 FIs rating it as effective or very effective (Figure 20).

Figure 20: Effectiveness of Device Fingerprinting



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Many solution providers offer device fingerprinting capabilities, and some FIs perform this identification in-house. Table C shows some of the leading device fingerprinting solution providers.

Table C: Leading Device Fingerprinting Solution Providers

Solution provider	Headquarters
41st Parameter, an Experian company	Scottsdale, Arizona
Entrust Datacard	Minneapolis
IdentityMind	Palo Alto, California
InAuth, an American Express company	Boston
iovation	Portland, Oregon
Kount	Boise, Idaho
Neustar	Sterling, Virginia
NuData, a Mastercard company	Vancouver, Canada
Oracle	Redwood City, California
RSA Security	Bedford, Massachusetts
Simility	Palo Alto, California

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

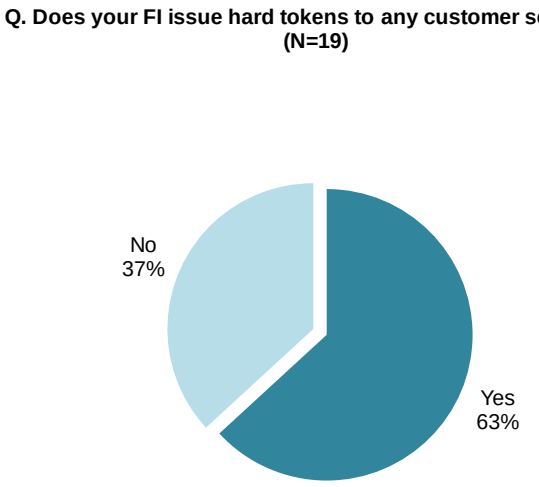
Solution provider	Headquarters
ThreatMetrix	San Jose, California
TRUSTID	Lake Oswego, Oregon
Vasco	Oakbrook Terrace, Illinois

Source: Aite Group

HARD TOKENS

Hard tokens have been used for many years to help protect online sessions, both for employees working remotely and for certain customer segments. Primarily, FIs offer hard tokens to their corporate customers, but hard tokens may also be offered to certain consumer segments, such as high-net-worth individuals. Only 63% of FIs currently offer hard tokens to any customer segment (Figure 21).

Figure 21: FI Issuance of Hard Tokens

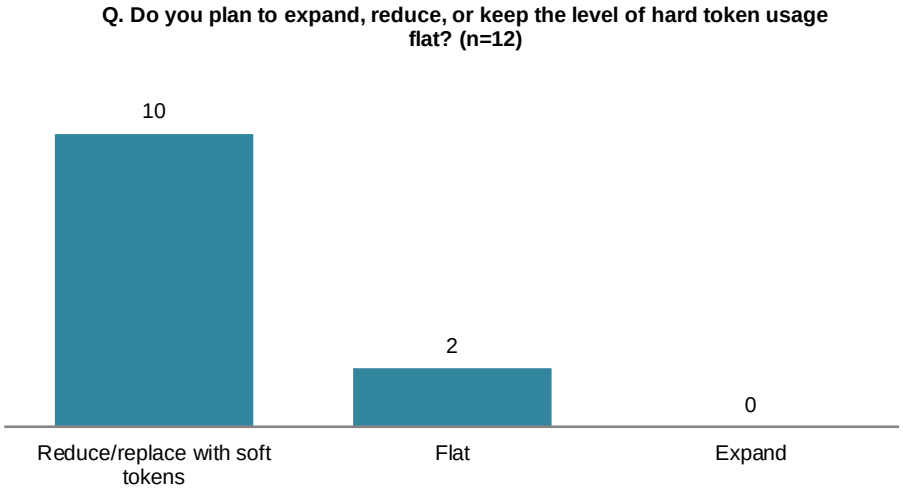


Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

The use of hard tokens is diminishing fairly rapidly (Figure 22). Only two FIs plan to keep their use of hard tokens flat going forward. All others anticipate reducing the use of hard tokens or replacing them entirely with soft tokens. The FIs that currently issue hard tokens to some consumer segments plan to replace them with the use of OOBA and OTPs. Mobile devices are increasingly playing a significant role in securing all customer activity regardless of the channel being used.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

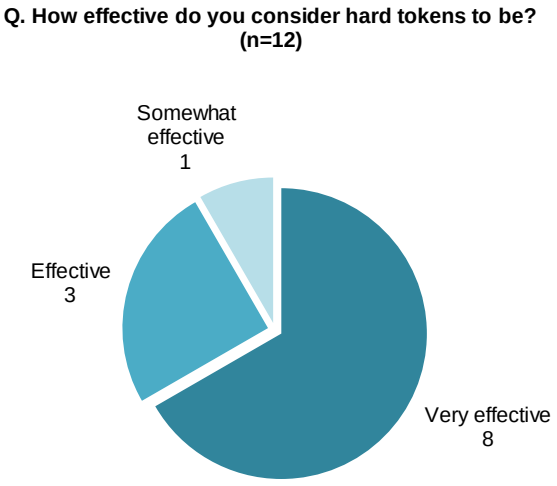
Figure 22: Planned Use of Hard Tokens



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

While the majority of FI executives who are at FIs that still use hard tokens consider them to be highly effective, they are quick to point out these devices' shortcomings. Customers sometimes forget them or lose them. They are very expensive and entail a great deal of friction. Lastly, they are susceptible to targeted attacks, leading one executive to rank them as only somewhat effective (Figure 23).

Figure 23: Effectiveness of Hard Tokens



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

KNOWLEDGE-BASED AUTHENTICATION

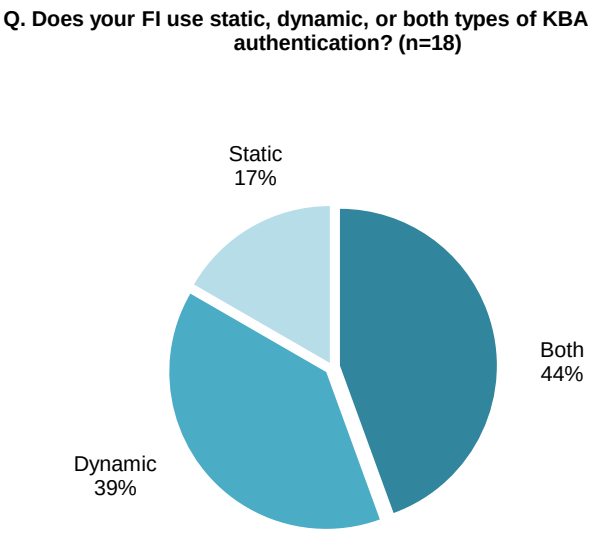
KBA or out-of-wallet questions have been used for decades as a method of using a shared secret or publicly available information to determine that the person is who he or she claims to be. Due to myriad data breaches, phishing attacks, and social engineering techniques used in contact centers, dedicated fraudsters can often supply correct answers to these questions. If the difficulty of the questions becomes too hard (in an attempt to defeat fraudsters), legitimate customers often cannot answer them.

KBA questions can be static (i.e., secret questions and answers arranged in advance for this purpose) or dynamic (i.e., credit or demographic-based questions asked of a consumer). Dynamic KBA is often provided by a vendor accessing public records or a credit bureau utilizing credit file data.

Regulators sometimes discourage the use of static questions, but the FIs interviewed say they can be quite effective if changed periodically. Some of the FIs that use static KBA describe an in-house solution whereby clients choose specific questions and supply answers; these questions must be updated quarterly. FIs that use both static and dynamic KBAs often use them for different use cases (e.g., using static questions for existing customers and using dynamic KBA for applicants for new accounts or cards).

Forty-four percent of FIs currently use both static and dynamic KBA; 39% use dynamic KBA only, and 17% use static KBA only (Figure 24).

Figure 24: FI Use of KBA for Online Authentication



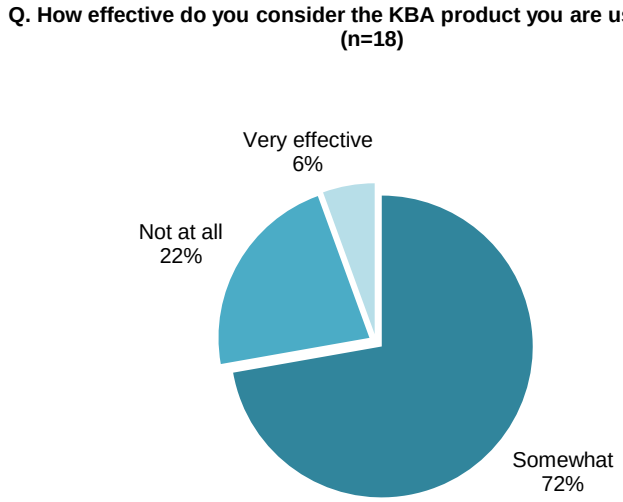
Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

The majority of FI executives (72%) state that KBA is only somewhat effective (Figure 25). Organized fraud rings have more access to data nowadays than ever before thanks to all the breaches. The data enables fraudsters to defeat the KBA questions (particularly when combined with social engineering tactics in contact centers), and legitimate customers often have trouble

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

answering the questions correctly. This combination makes it increasingly difficult to justify the high level of customer friction KBA entails.

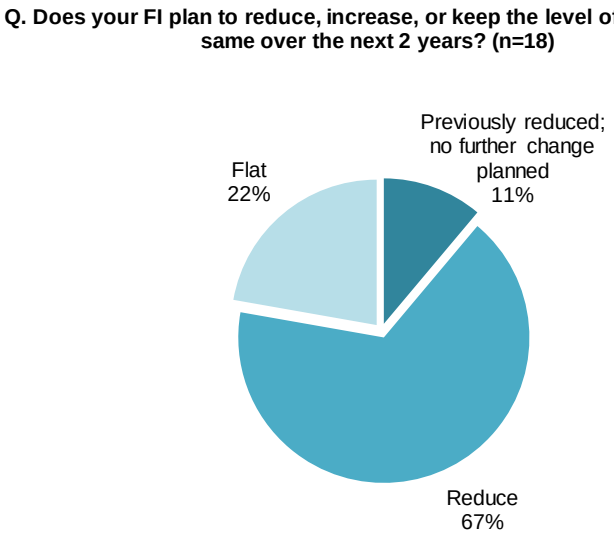
Figure 25: KBA Effectiveness



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Eleven percent of FIs have reduced the level of KBA used in recent years and have no plans to reduce it further. Usage will remain flat at 22% of FIs in the next two years, while 67% plan to reduce KBA usage (Figure 26). Most of the executives state they will not totally eliminate the use of KBA, while others do plan to replace it entirely with OTPs and biometric solutions.

Figure 26: Changes Planned for KBA Use in Next Two Years



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

There are many KBA vendors; Table D shows some of the leading providers in the U.S. market.

Table D: Leading KBA Solution Providers in the U.S.

Solution provider	Headquarters
Acxiom	Little Rock, Arkansas
Equifax	Atlanta
Experian	Dublin, Ireland
FIS	Jacksonville, Florida
ID Analytics	San Diego, California
IDology	Atlanta
LexisNexis Risk Solutions	Alpharetta, Georgia
RSA Security	Bedford, Massachusetts
TransUnion	Chicago

Source: Aite Group

ONLINE CREDENTIALS

While many FI executives bemoan automated attacks that use username and password combinations from various data breaches to identify FI sites where the combinations work, all FIs that participated in this research still use passwords as one layer of online security. Online credentials are not very secure given that many consumers use the same credentials for all online activity.[10] Even though it appears that passwords only give consumers a false sense of security, the industry is not yet ready to remove them from its arsenal of tools to protect digital channels.

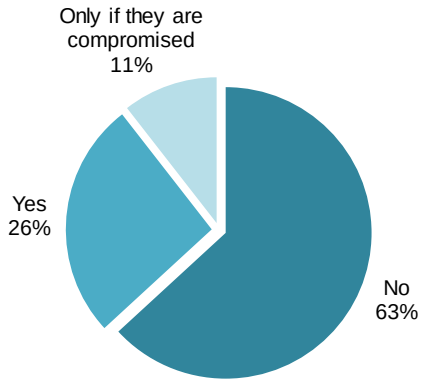
Only 26% of FIs require consumers to change their passwords periodically. Among that group, the most common time period for changes is every 90 days. Another 11% of FIs comment that they don't usually require password changes, but if they are aware that the password has been compromised, of course they require the customer to change it. The majority (63%) have no requirement for consumers to change passwords periodically (Figure 27).

10. See Aite Group's report *Second Annual Global Security Engagement Scorecard™*, October 2017.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 27: Requirements to Periodically Change Passwords

Q. Are there any requirements for retail clients to change the password periodically? (N=19)

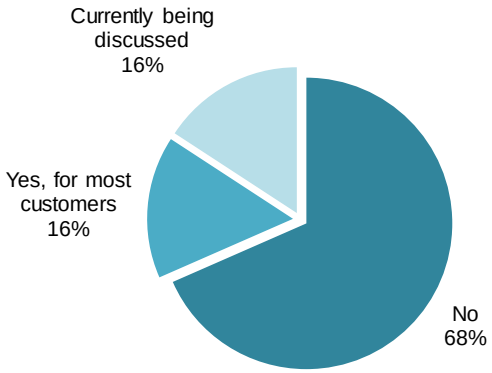


Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Executives lack faith in passwords, and many state they would like to discontinue using them, but most do not have firm plans to do so. Sixty-eight percent of FIs state they have no plans to phase out passwords or that they plan to do so but that it will take longer than two to three years. Sixteen percent state that they have plans to phase out the use of passwords for about 95% of their customers; the passwords will be replaced by OTPs and various forms of biometrics. (There will still be a small minority of customers who do not use smartphones, so those customers will continue to use passwords.) The remaining 16% say there are discussions going on currently within their FIs but that no firm decision has been made on this issue yet (Figure 28).

Figure 28: Plans to Phase Out Passwords

Q. Does your FI plan to phase out passwords in the next 2 to 3 years or less for online, mobile, or both? (N=19)

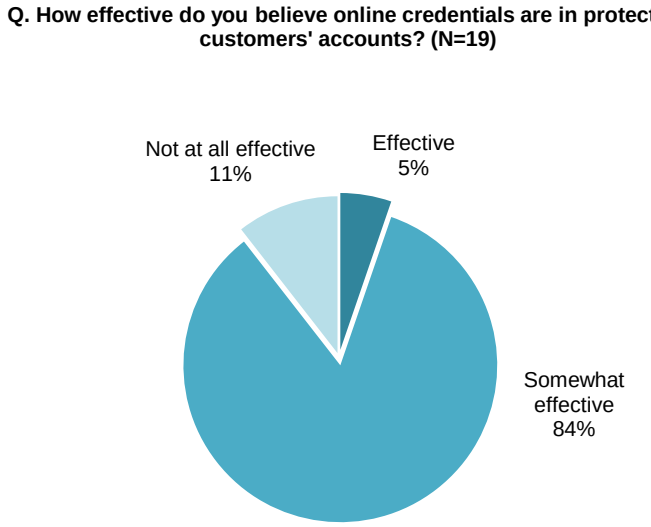


Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Given that the majority of FIs do not plan to phase out passwords in the next two to three years, it is interesting to note that executives place so little confidence in passwords' ability to protect customers' accounts. Eleven percent of executives state that online credentials are not at all effective in protecting customers' accounts. The vast majority (84%) state that online credentials are only somewhat effective. One respondent, representing 5% of the sample, considers them effective but sarcastically adds "until there is a data breach or bot attack" (Figure 29).

Figure 29: Effectiveness of Online Credentials



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

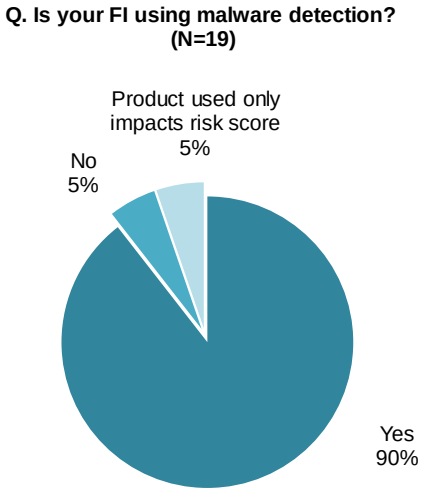
MALWARE DETECTION

Malware represents risk in both the online and mobile channels, but those risks are much higher in the online channel. Similarly, risks are higher on commercial accounts than on consumer ones, since transactions tend to be of larger dollar amounts for businesses.

The majority of FIs (90%) use malware detection at a minimum for commercial accounts. Some also use malware detection on the small-business account portfolio that uses wire and ACH services, and a few extend the protection to some or all consumer accounts. Also, one FI, representing 5% of the sample, uses a form of malware detection that doesn't add any value other than providing input to a model that calculates the risk score for transactions (Figure 30).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 30: FI Use of Malware Detection Products



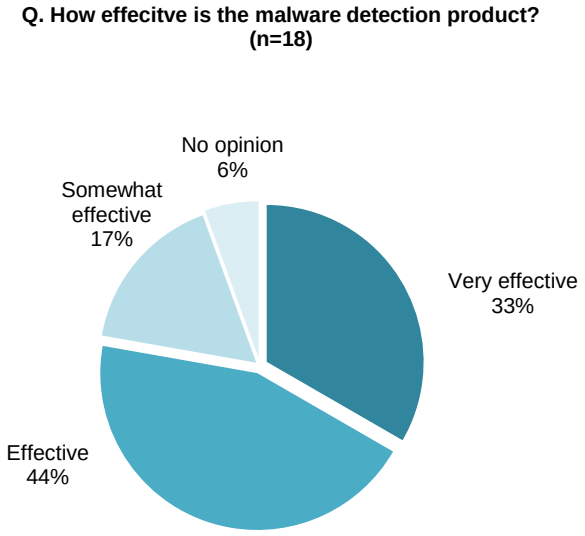
Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

FIs that use malware detection often require commercial clients to use the products; if malware is detected, the vendor can assist with removing the malware. While this is very helpful, the same service is not always offered to consumers. One executive mentions that the presence of malware doesn't mean that it is malicious and that the high false-positive rate due to malware that offers little risk is a major challenge for consumer accounts.

Opinions regarding the effectiveness of malware detection products vary, but they are overall positive. The one FI that does not use malware detection used it previously but dropped it due to poor acceptance rates. Some executives comment that malware detection is only worthwhile if you diligently keep the software current. Others comment that the alerts they receive are not as timely as they desire and that the product they use has no interdiction capability. One executive comments that the product is very effective on the commercial side but only somewhat effective on the consumer side; another executive comments that he would need an army of analysts to follow up on all the alerts received on consumer accounts. One executive states that he cannot provide an opinion because his FI has not yet tracked the effectiveness of the product (Figure 31). Malware detection solution providers include F5, IBM, InAuth, RSA Security, and ThreatMetrix.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 31: Effectiveness of Malware Detection

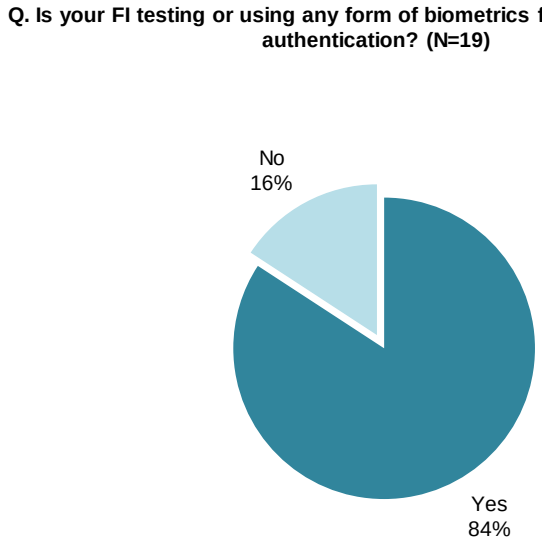


Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

BIOMETRICS

In recent years, FIs have begun using a variety of biometrics, including voice biometrics in contact centers and various forms of biometrics in the mobile channel. The use of some biometrics is facilitated by smart devices, while others are actively or passively collected and used for fraud prevention purposes. A large majority (84%) of FIs are using at least one type of biometric to help authenticate customers (Figure 32).

Figure 32: Use of Biometrics at Large FIs

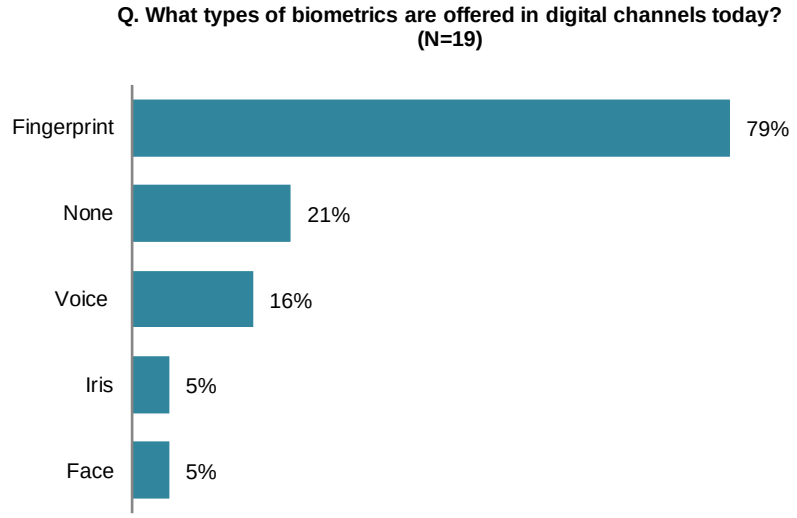


Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Fingerprints are by far the most commonly accepted biometric; 79% accept a fingerprint used on a device in digital channels. Voice is the next most commonly accepted, at only 16% of FIs. Iris and face are just beginning to be accepted, but usage will grow as handset manufacturers build these features into devices (Figure 33).

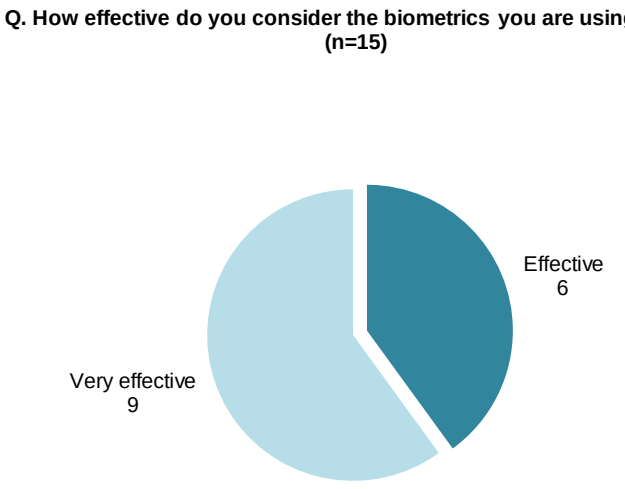
Figure 33: Types of Biometrics Offered by Large FIs



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Overall, executives express very high confidence in biometrics as part of the authentication process. The majority state biometrics are very effective, and the rest state they are effective. Not a single executive could recall an instance when fraud resulted from the use of a biometric (Figure 34).

Figure 34: Effectiveness of Biometrics



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Leading FIs are following handset manufacturers' developments carefully and plan to incorporate handsets' biometrics into their authentication strategies.[11] This allows them to use biometrics to authenticate customers via mobile devices but avoid the expense of developing and maintaining biometric databases and the risk that such a database could be breached. In addition, they can avoid the risk of future regulatory oversight that could curtail the use of biometrics they collected and the potential of a consumer backlash.

There are many solution providers in the biometrics space; Table E shows leading providers of biometrics.

Table E: Leading Biometrics Solutions Providers

Solution provider	Headquarters
Agnitio	Madrid, Spain
Aware	Bedford, Massachusetts
BioConnect	Toronto, Ontario, Canada
BioTrust	Amsterdam, The Netherlands
Daon*	Reston, Virginia
Delta ID	Newark, California
Early Warning Services*	Scottsdale, Arizona
EyeVerify	Kansas City, Missouri
Facebanx	London, England
Fujitsu	Minato, Tokyo, Japan
Gemalto	Amsterdam, The Netherlands
GreenKey	Jersey City, New Jersey
Hitachi	Chiyoda, Tokyo, Japan
Hypr	New York, New York
LexisNexis Risk Solutions	Alpharetta, Georgia
NEC	Minato, Tokyo, Japan
Nice Systems	Ra'anana, Israel
Nok Nok Labs	Palo Alto, California
Nuance	Burlington, Massachusetts

11. Penny Crosman, "The Eyes Have It: Bank of America, Samsung Pilot Iris-Scan Logins," American Banker, August 8, 2017, accessed November 3, 2017, https://www.americanbanker.com/news/the-eyes-have-it-bank-of-america-samsung-pilot-iris-scan-logins.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Solution provider	Headquarters
Nymi	Toronto, Ontario, Canada
OneVisage	Lausanne, Switzerland
OT-Morpho	Paris, France
Pindrop Security	Atlanta, Georgia
RSA Security*	Bedford, Massachusetts
SayPay Technologies	El Segundo, California
Sensory Technologies	Indianapolis, Indiana
Sestek	Istanbul
ValidSoft	Tullamore, Ireland
Vasco	Oakbrook Terrace, Illinois
Verint Systems*	Huntington, New York
Voice Biometrics Group	New Town, Pennsylvania
VoicePIN	Krakow
VoiceVault	El Segundo, California

Source: Aite Group
**Indicates that the solution is white-labeled and is provided by another vendor*

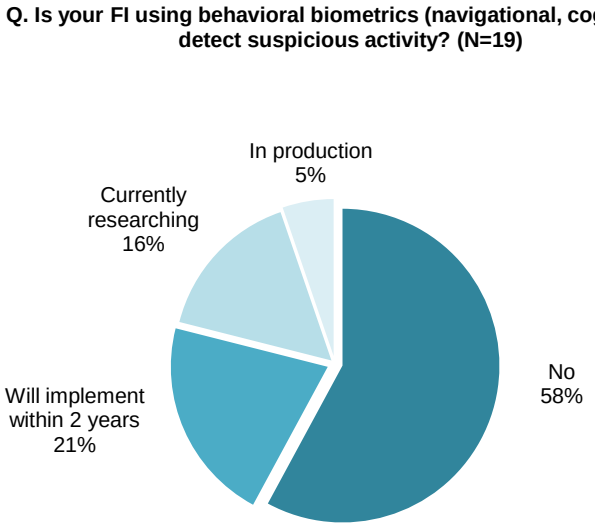
BEHAVIORAL BIOMETRICS

Initially, behavioral biometrics were used predominantly to analyze the ways consumers entered data on devices and interacted with devices. By establishing unique patterns for each customer, behavioral biometrics can detect when someone else is accessing an account instead of the customer. The use of behavioral biometrics has extended to the application fraud use case by distinguishing between a normal applicant's behavior and that of a fraudster based on the way data is entered on an application. In addition, these solutions can distinguish between human behavior and that of automated bots attempting to access accounts.

Behavioral biometrics as a product is relatively new to the market and, therefore, has not been adopted heavily yet. Only 5% of FIs participating in this research have behavioral biometrics in production; another 21% say they will implement behavioral biometrics within the next two years, and 16% are currently researching such products. Fifty-eight percent of participating FIs are not yet researching or using behavioral biometrics (Figure 35). This is indicative of a market in which leading-edge FIs have not yet strongly endorsed the effectiveness of such products; once they do, adoption by fast followers will surely occur.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 35: Use of Behavioral Biometrics by Large FIs



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

While the use of behavioral analytics is a relatively new method of detecting fraud, several companies offer the capability, and more are sure to do so in coming years. Table F shows leading solution providers of behavioral biometrics.

Table F: Leading Behavioral Biometrics Solution Providers

Solution provider	Headquarters
AimBrain	London
BehavioSec	Stockholm
BioCatch	Tel Aviv
Experian, via Biocatch	Dublin
InAuth, an American Express company	Boston
Kofax	Irvine, California
Neuro-ID	Whitefish, Montana
NuData Security, a Mastercard company	Vancouver, Canada
SecuredTouch	Palo Alto, California
ThreatMetrix	San Jose, California
VASCO	Oakbrook Terrace, Illinois

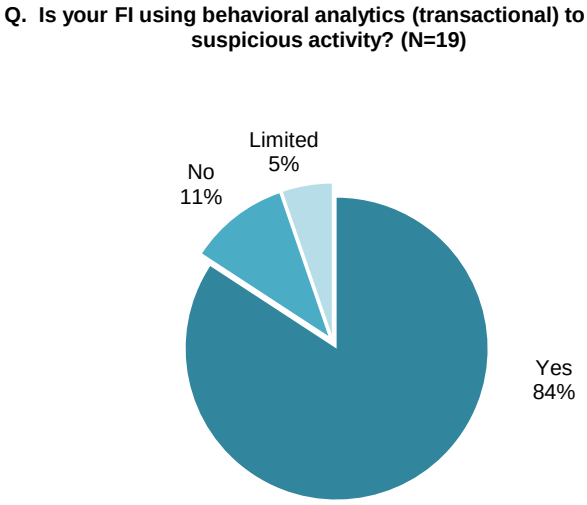
Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

BEHAVIORAL ANALYTICS

Behavioral analytics have existed in the market much longer than behavioral biometrics and have seen much more adoption; behavioral analytics examine the patterns of transactional activity that are normal for a specific customer and identify anomalies. Eighty-four percent of FIs are currently using at least one type of behavioral analytics to detect suspicious activity; 5% state they are using them in a limited way (Figure 36).

Figure 36: Use of Behavioral Analytics by Large FIs

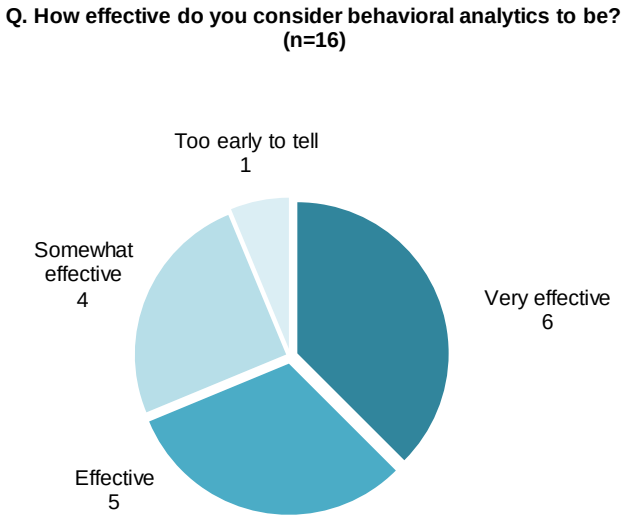


Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

The majority of FIs (11 out of 16) find behavioral analytics to be effective or very effective in combatting fraud. An additional four FIs find them to be somewhat effective (Figure 37). Usage of behavioral analytics varies, with some FIs primarily using them to detect suspicious activity in the card space and others using them broadly over many use cases, such as wire, ACH, card, logins, and account maintenance transactions. Some of the FIs indicate that they plan to build internal capabilities to use behavioral analytics or have recently done so. These FIs indicate plans to use behavioral analytics far more extensively in the future than they do today.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 37: Effectiveness of Behavioral Analytics



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

Many solution providers offer behavioral analytics solutions to detect anomalies and other suspicious activity. Table G lists some of the leading firms in this space.

Table G: Leading Behavioral Analytics Solution Providers

Solution provider	Headquarters
ACI Worldwide	Naples, Florida
BAE Systems	London
BehavioSec	Stockholm
BioCatch	Sweden
Brighterion	San Francisco
CardinalCommerce	Mentor, Ohio
DataVisor	Mountain View, California
Easy Solutions	Doral, Florida
Feature Analytics	Nivelles, Belgium
Feedzai	San Mateo, California
FICO	San Jose, California
FIS	Jacksonville, Florida
Fiserv	Brookfield, Wisconsin
Guardian Analytics	Mountain View, California

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Solution provider	Headquarters
IBM	Armonk, New York
Intellinx, a Bottomline Technologies company	Or-Yehuda, Israel
iSoft	Banbury, U.K.
Jack Henry	Monett, Missouri
Nice Actimize	New York
NuData Security, a Mastercard company	Vancouver, Canada
Oracle	Redwood City, California
Risk Ident	
RSA Security	Bedford, Massachusetts
SAS	Cary, North Carolina
Simility	Palo Alto, California
ThetaRay	Hod HaSharon, Israel
ThreatMetrix	San Jose, CA
Wipro	Bengaluru, India

Source: Aite Group

The second report in this two-part series will be published shortly; it will focus on external and internal factors that are influencing FIs' digital channel fraud mitigation strategies.

:

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RECOMMENDATIONS

Protecting the digital channels is vitally important, particularly in the current environment where threats increase and morph constantly. Here are a few recommendations for players in the space.

FIs:

- Evaluate authentication processes enterprise-wide to detect gaps.
- Consider new authentication methods that offer improved results with less negative impacts (friction) for customers.
- Evaluate authentication methods that do not rely on data that is readily available to fraudsters; ensure that at least one layer of your security utilizes such a method.

Solution providers:

- Evaluate products for the level of customer friction introduced; reduce friction wherever possible.
- Where possible, ensure products meet the current needs in the market (e.g., if you offer identity products, ensure they have elements that make it difficult for fraudsters to circumvent them).
- Understand the types of fraud challenges FIs are facing and ensure your salespeople can speak the language of the executives they are selling to.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

Digital Authentication: New Opportunities to Enhance the Customer Journey, September 2017.

Financial Institution Fraud Trends: ATO and Application Fraud Rising Rapidly, May 2017.

FFIEC and NIST Guidance: Mobile and Digital Requirements, April 2017.

ATM Fraud: Increasingly Organized, November 2016.

Contact Centers: The Fraud Enablement Channel, April 2016.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

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
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT EARLY WARNING

Creating the Future of Payments®

Early Warning delivers innovative payment and risk solutions to financial institutions nationwide.

For over 25 years, Early Warning has been a leader in technology that helps protect and advance the financial system. We serve a diverse network of approximately 2,500 financial institutions, government entities and payment companies. Our product solutions enable real-time funds availability for a variety of payment types through our payments network.

For more information, visit www.earlywarning.com.

ABOUT ZELLE®

Brought to you by Early Warning Services, LLC, an innovator in payment and risk management solutions, *Zelle* makes it easy, fast and safe for money to move. The Zelle Network® connects the nation's leading financial institutions, *enabling consumers* to send fast person-to-person payments to nearly anyone with a bank account in the U.S. Funds are available directly in consumer bank accounts generally within minutes when the recipient is already enrolled with *Zelle*. To learn more about *Zelle* and its participating financial institutions, visit http://www.zellepay.com.

SOLUTIONS TO HELP SECURE DIGITAL PAYMENTS

Consumer expectations for immediacy are driving changes in the payments industry; as payments migrate to real-time, it is important that fraud and risk mitigation tools also keep pace.

The *Zelle Network* enables easy, fast and safe money movement through three unique use cases - Person-to-Person (P2P), Corporate & Government Disbursements (B2C) and Small Business.

- *Zelle* P2P: Through the convenience of mobile banking apps, *Zelle* P2P is a way for consumers with a U.S. bank account to send and receive money with almost anyone they know, using simply a mobile number or email address.
- *Zelle* Disbursements: Corporate and government disbursements give financial institutions a solution for reducing check expenses and growing revenue within treasury groups, while giving businesses the capability to disburse funds straight to their customer's account without requesting or storing sensitive bank account information.
- *Zelle* Small Business: Changing the way small businesses can send, receive and request payments. *Zelle* Small Business allows consumers an easier way to move money to their gardeners, hair stylists, dog walkers and other goods and services providers that they trust.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Early Warning provides authentication solutions to validate people, devices and transactions associated with faster payments by:

- Verifying that the device and phone enrolling on the network are tied to your customer
- Providing frictionless authentication to protect against unauthorized transactions and login
- Validating contact information provided when changes are made to a user profile
- Authenticating receiver phone number is trustworthy to ensure funds are sent to the correct recipient
- Ensuring notifications and text messages are received by the intended recipient
- Confirming the phone number/token is accurate and up-to-date

To learn more about Early Warning, visit EarlyWarning.com

or contact an Early Warning Account Manager

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com