Aite PARTNER. ADVISOR. CATALYST.

Market Trends in Digital Fraud Mitigation

DECEMBER 2019

Trace Fooshée

NUANCE®

This report, licensed for distribution and provided compliments of Nuance Communications, Inc., is an independent syndicated research report produced by Aite Group LLC.

TABLE OF CONTENTS

IMPACT POINTS 4
INTRODUCTION 5
METHODOLOGY 5
THE MARKET 7
DRIVERS AND CHALLENGES 8
PRESSURE TO IMPROVE CLIENT EXPERIENCE IS INCREASING 8
EXPANSIONS IN DIGITAL SALES AND SERVICE PLATFORMS 11
DIGITAL FRAUD TRENDS 15
PRIORITIES 19
CONTROLS THAT HAVE OUTLIVED THEIR UTILITY 20
CONTROLS THAT ARE WORKING WELL 23
ORCHESTRATION HUBS AND OTHER EMERGING SOLUTIONS 24
CONCLUSION 26
RELATED AITE GROUP RESEARCH 27
ABOUT AITE GROUP 28
AUTHOR INFORMATION 28
CONTACT 28

LIST OF FIGURES

FIGURE 1: ASSET SIZE OF PARTICIPATING FIS 6
FIGURE 2: RATE OF INCREASE IN DIGITAL FRAUD ATTACKS AND LOSSES 8
FIGURE 3: THE FRAUD BALANCING ACT 9
FIGURE 4: RELATIVE WEIGHT OF IMPORTANCE OF CLIENT EXPERIENCE IN JUSTIFYING INVESTMENT 10
FIGURE 5: DIGITAL FRAUD BUDGET INCREASES 10
FIGURE 6: AUTHENTICATION TRANSFORMATION A REFLECTION OF FI STRATEGIC PRIORITIES 11
FIGURE 7: BUDGET COMPARISONS—DIGITAL SALES AND SERVICE PLATFORMS VERSUS DIGITAL FRAUD MITIGATION 12
FIGURE 8: LINKAGE BETWEEN DIGITAL SALES AND SERVICE PLATFORM GROWTH AND DIGITAL FRAUD... 12
FIGURE 9: DIGITAL FRAUD WITH A CALL CENTER COMPONENT 13
FIGURE 10: IMPACT OF DIGITAL FRAUD ON CALL CENTER VOLUME AND COST 13
FIGURE 11: DIGITAL SERVICES BEHIND DIGITAL FRAUD ATTACK RATE INCREASES 14
FIGURE 12: FRAUD-RELATED ONLINE AND MOBILE APP FUNCTIONALITIES IMPACTING CLIENT EXPERIENCE 15
FIGURE 13: ACH ATO SCHEME 16
FIGURE 14: THE IMPACT OF SIM SWAPPING 17
FIGURE 15: FIRST-PARTY CHECK FRAUD GROWTH AND LINKAGE WITH DIGITAL SALES AND SERVICE PLATFORMS 18
FIGURE 16: PLANS TO PHASE OUT PASSWORDS 21

FIGURE 17: PLANS TO PHASE OUT KBA 22
FIGURE 18: ADOPTION PATTERNS OF OTP 23
FIGURE 19: ADOPTION PATTERNS OF AUTHENTICATION CONTROLS 23
FIGURE 20: EFFECTIVENESS OF AUTHENTICATION CONTROLS 24
FIGURE 21: AUTHENTICATION HUB ADOPTION 25

LIST OF TABLES

TABLE A: THE MARKET........ 7
TABLE B: CHALLENGES AND IMPLICATIONS OF FORMULATING A DIGITAL FRAUD MITIGATION ROADMAP 19

IMPACT POINTS

- This Impact Report examines market trends impacting how large financial institutions (FIs) are balancing security and the client experience as they navigate the expansive digital transformation initiatives that are common across the industry today. It is based on interviews with FI executives among 18 of the 40 largest North American FIs.
- Fraud executives are under extraordinary pressure to balance client experience and loss mitigation, but with this pressure comes opportunities to leverage significant sources of support and, potentially, funding for initiatives that serve to improve loss mitigation as well as client experience.
- Gaps between how FIs in the industry balance investments in digital security and how they balance those in digital client experience are amplified, and those that don't prioritize security are unwittingly contributing to increases in financial crime across the industry.
- Digital fraud continues to expand in scope and sophistication, necessitating ever-greater demand for more capable and flexible fraud detection solutions that are as capable of detecting and preventing fraud as they are of paving the way for smoother client experiences.
- Though general consensus among security professionals and fraud executives contradicts the use of passwords and knowledge-based authentication (KBA), most FIs continue to depend on these security controls to protect their digital channels.
- The demand for more sophisticated authentication and transaction monitoring controls to compensate for increasing rates of digital fraud attacks and losses has indicated that some authentication controls are enjoying greater adoption and success than others.

INTRODUCTION

The global trend to digitize banking services plays as important a role as ever among North American banks' strategic priorities, and efforts to expand digital sales and service platforms are still accelerating. As banks continue to aggressively expand these digital sales and service platforms, including innovations in payment services, they're inadvertently creating vulnerabilities that are fueling the growth of financial crime. While a wider variety of powerful security solutions is available than ever before, many of which are tailored exclusively for mitigating risks specific to digital channels, not all banks are prioritizing investments in those security solutions as highly as investments in expanding digital sales and service platforms. The gaps that have long existed between those banks and those that prioritize investment in security solutions equally with investments in digital sales and service solutions are growing wider, and this, too, is driving growth in digital fraud.

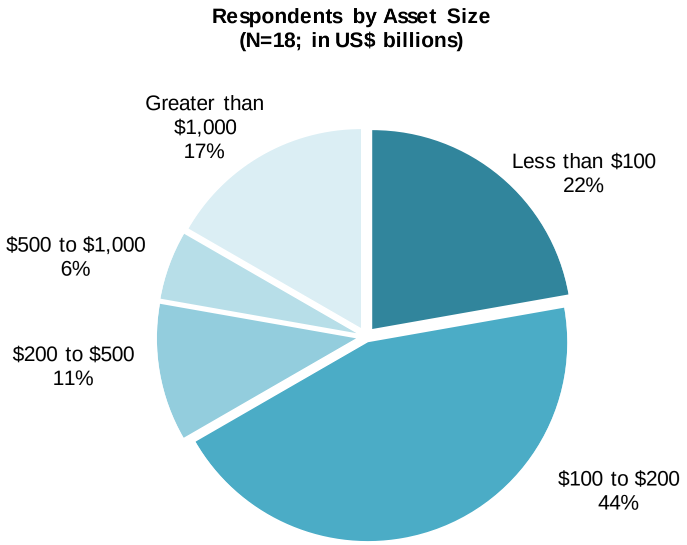
This Impact Report examines the drivers behind digital fraud trends, the challenges that fraud executives face in controlling digital fraud, and how those drivers and challenges are impacting how they prioritize the investments that they're eager to make to mature their ability to protect their bank and their clients from fraud in digital channels. As a follow-up to a previous report published in 2017,[1] this report also examines the relative degree of satisfaction that fraud executives in the industry report with regard to the effectiveness of various controls as well as where they're placing their bets on emerging technologies.

METHODOLOGY

Aite Group devised a series of 54 survey questions that were distributed to 20 fraud and digital channel executives from 18 North American FIs that have more than US$25 billion in assets from July to October 2019. The responses to the survey questions were collected and augmented with telephone interviews and emailed follow-up questions. Eight of the banks operate exclusively in the U.S., and the other eight banks operate in international markets. Figure 1 shows the breakdown of participating FIs by asset size.

[1] See Aite Group's report *Digital Channel Fraud Mitigation: Market Trends Influencing FI Strategies*, November 2017.

Figure 1: Asset Size of Participating FIs



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

THE MARKET

The strategies being developed by FIs to protect digital channels in the future are being impacted by many changes in the market. Table A lists several of the influencing factors in the current market that are examined in this report.

Table A: The Market

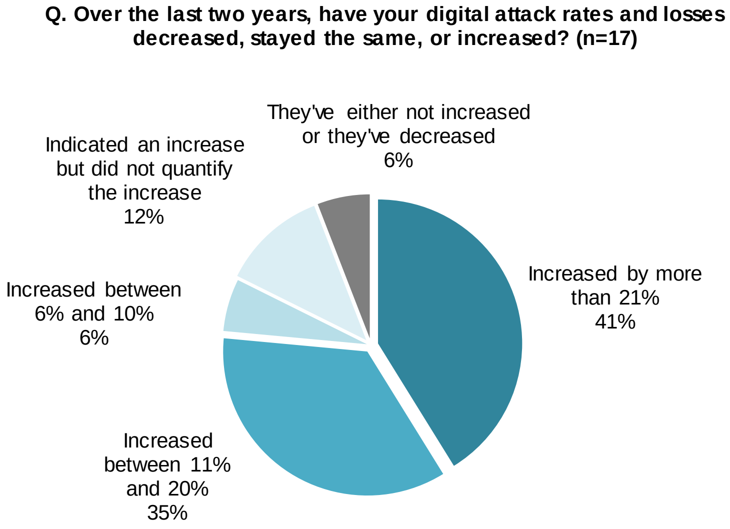
Market trends	Market implications
Convenience, usability, and innovative services, such as faster payment options, are driving growth in digital channels.	The anonymity of services offered through digital channels as well as the opportunities for automating their abuse make these services popular targets for financial criminals.
FIs are expanding the scope of digital sales and service features to meet consumer demand and to match or exceed digital services on offer from fintech challengers.	FIs that fail to deploy a robust and thoughtfully architected control framework to support the rapid expansion of digital sales and service offerings are more likely than their peers to suffer disproportionately high rates of financial crime.
The pressure to reduce friction in digital channels is amplifying the market for authentication and identity verification solutions.	Many FIs are justifying increased investments to renovate or transform their authentication and identity verification controls with more emphasis than ever on the objective of improving client experience and/or increased acquisition rates.
Authentication hubs have emerged as popular solutions to improve the effectiveness, efficiency, and client experience associated with authentication controls.	As the quantity and complexity of identity verification controls proliferate to counter growing threats, such as account takeover (ATO), application fraud, mule activity, and first-party check fraud, it's likely that the scope of authentication hubs will expand to orchestrate identity verification controls.
As digital fraud tactics evolve and mature, many of them, such as ATO, are becoming industrialized thanks to automation.	The volatile nature of industrialized and highly automated digital fraud attacks can cause substantial disruptions in supporting business units (specifically, contact centers) in such a way that can amplify losses and exacerbate customer attrition for those that fail to plan properly.
Innovations such as faster payments are expected to amplify fraudulent activity and to exert influence over the need for greater cooperation between fraud and anti-money laundering operations.	FIs need to develop robust and thoughtfully designed policies, operations, and detection and case management infrastructure to manage increases in mule activity and to take decisive, accurate, defensible, and swift action on suspicious inbound payments.

Source: Aite Group

DRIVERS AND CHALLENGES

The expectations of those who manage fraud operations units in most FIs today are as complex and challenging as they have ever been. Fraud executives are expected to reduce fraud losses while simultaneously making significant improvements to client experience, and with rigorously scrutinized budgets. In parallel with these objectives, these fraud executives are expected to manage a variety of processes that are, for many FIs, still largely manual, within increasingly restrictive compliance requirements—all of this despite double-digit growth in fraud attack rates and losses (Figure 2) and a constantly expanding and ever-evolving digital surface area to defend and protect.

Figure 2: Rate of Increase in Digital Fraud Attacks and Losses

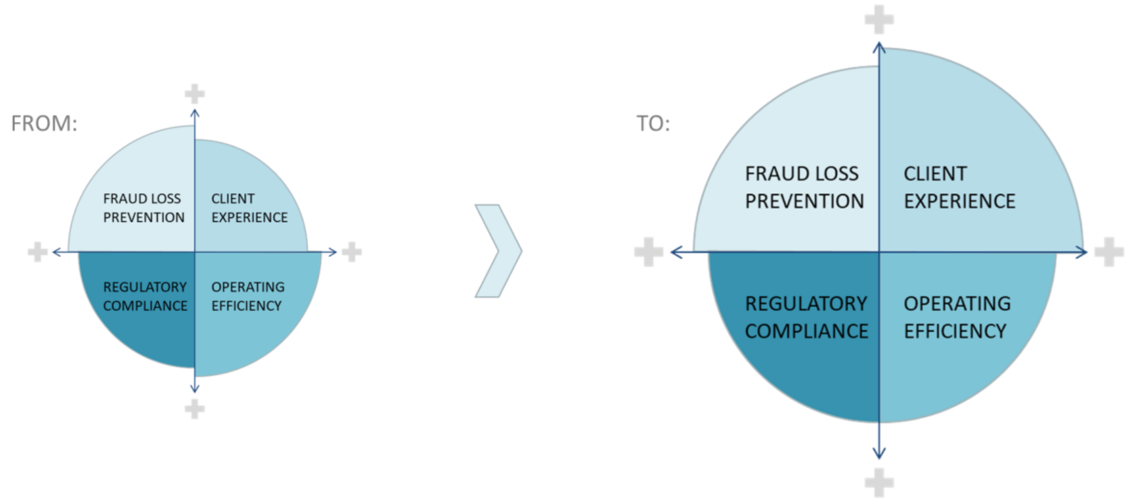


Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

PRESSURE TO IMPROVE CLIENT EXPERIENCE IS INCREASING

The objective and dynamics of balancing losses, client experience, regulatory compliance, and operating efficiency is fundamentally the same today as it always has been. The collective pressure to contain losses, improve client experience, reduce cost, and maintain compliance has increased. Additionally, some domains have increased disproportionately greater than others (Figure 3). While the importance of maintaining compliance with Regulations E, Z, and CC—the Federal Reserve's guidance for compliance with the Electronic Fund Transfer Act, the Truth in Lending Act, and the Check Clearing for the 21st Century Act, respectively—has remained relatively constant, pressure to address consumer complaints and to demonstrate mastery of governance of the growing inventory of risk models that are permeating many FIs today have increased the weight of importance of maintaining regulatory compliance. The pressure to contain fraud losses is also a constant but made considerably more challenging in the context of double-digit growth in attack rates (Figure 2). The relative weight of importance in containing costs is, perhaps, the most variable from one FI to the next, but most FIs report that pressure to contain or reduce costs has steadily persisted or increased since 2008.

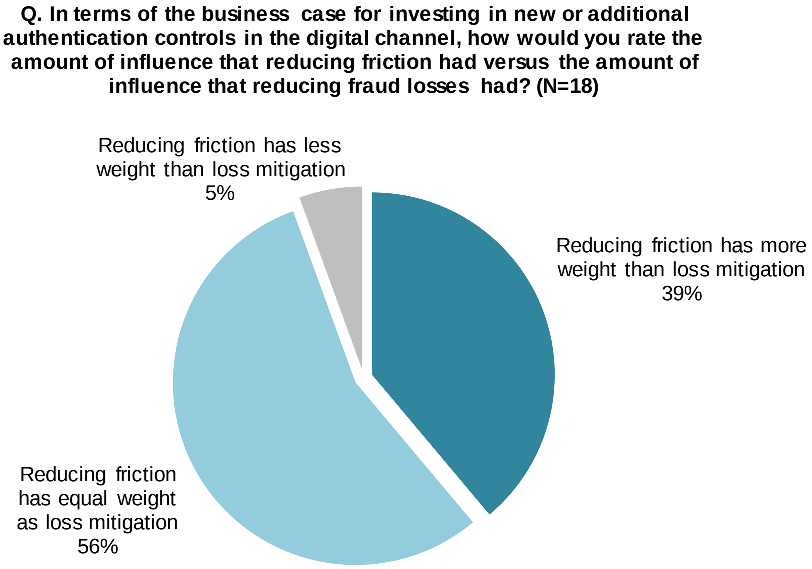
Figure 3: The Fraud Balancing Act



Source: Aite Group

The element of the balancing act that has seen the greatest increase in terms of relative weight of importance has been client experience. As banks race both competitors within the industry and fintech challengers, the relative weight of importance of creating engaging digital-first experiences has taken on significantly greater value. While this is certainly true as it pertains to prioritizing budget for investments in digital sales and service platforms, it's also having a profound impact on the dynamics of investment priorities in security-related business units. This is, perhaps, especially true for those business units that manage policies and processes that govern identity authentication and verification. Figure 4 illustrates the responses from fraud executives in describing the weight that client experience has in prioritizing and justifying investments in authentication controls in the digital channel relative to the weight of loss mitigation.

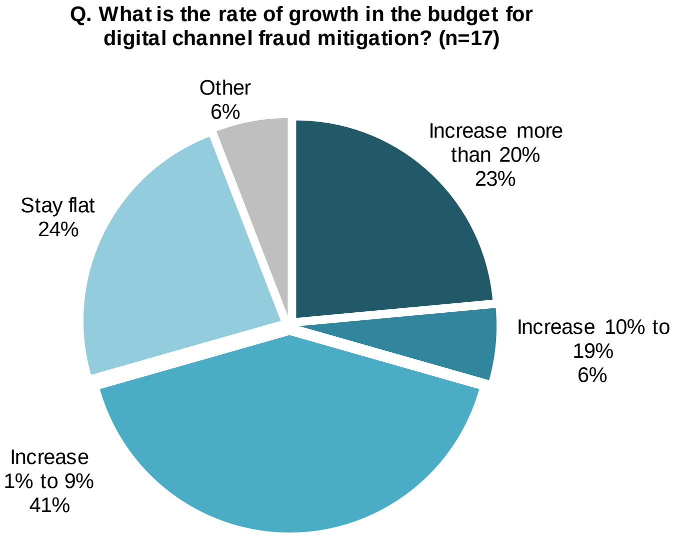
Figure 4: Relative Weight of Importance of Client Experience in Justifying Investment



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

That only one respondent out of 18 reports that client experience has less weight than loss mitigation illustrates the desire to improve the client experience in the digital channel is playing a significant role in investment decisions. Another perspective is that fraud executives are finding success in leveraging improvements to client experience in their business case justification more than ever (Figure 5). This trend has led to net increases in investment and operations budgets in recent years, although it is unclear whether these increases are derived primarily from mandates to reduce friction in authentication and identity verification or to combat increased attack rates.

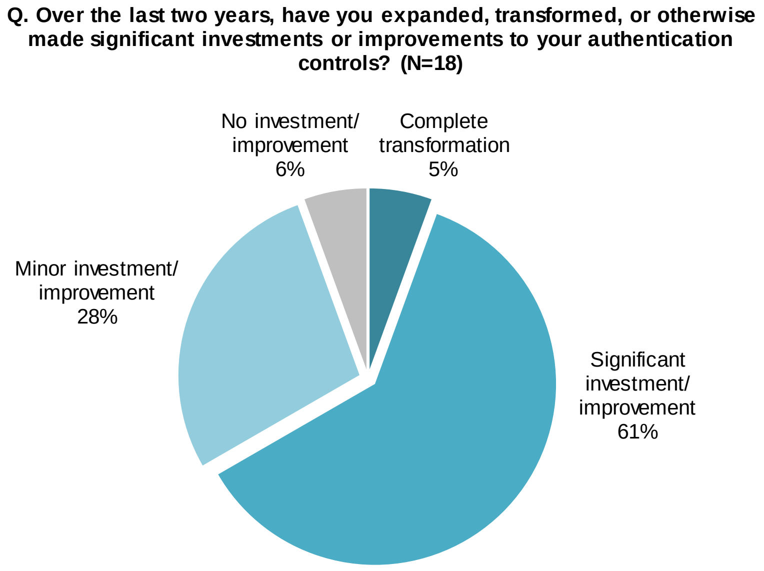
Figure 5: Digital Fraud Budget Increases



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

Regardless, the net increase in spending has given rise to a burgeoning landscape of software solutions that aim to improve the efficiency, effectiveness, and client experience related to various aspects of antifraud operations. Authentication and identity verification solution providers are among those that are enjoying the most robust growth rates. Two-thirds of respondents are either making significant improvements to their authentication control platforms or are completely transforming them (Figure 6). That only one respondent reported that they were not making any investments or improvements to their authentication controls lends evidence to the notion that most FIs have placed investments in authentication as a top priority.

Figure 6: Authentication Transformation a Reflection of FI Strategic Priorities

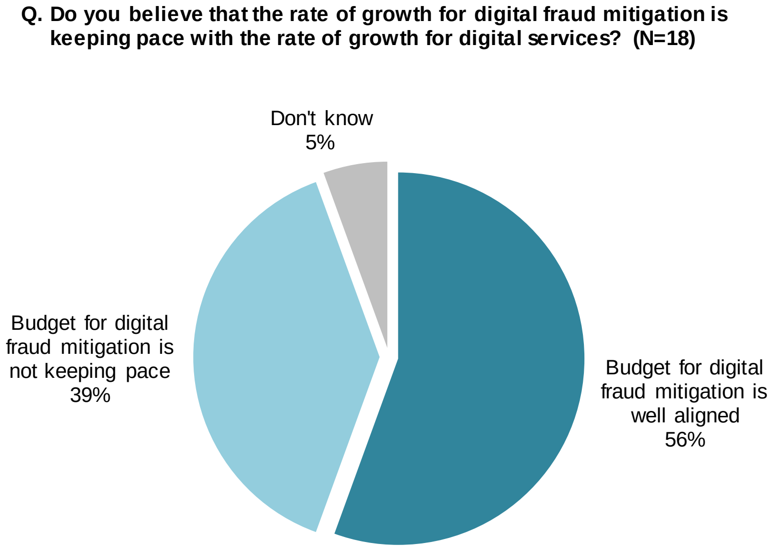


Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

EXPANSIONS IN DIGITAL SALES AND SERVICE PLATFORMS

While it’s clear that most of the top 40 U.S. banks are unanimous in placing the digitization of sales and service platforms at or among their primary strategic business objectives, it’s also evident that there are a variety of approaches to achieving those objectives. The larger banks in the top 40 enjoy greater economies of scale in their pursuit of digitization, albeit with the added challenge of larger and more complex ecosystems to transform. Banks in the middle tier have the advantage of less complex ecosystems to transform but are challenged by smaller capital reserves to fund their transformation initiatives. Most respondents report that their organizations prioritize these efforts equally; however, some report that investments in sales and service transformations are outstripping investments in digital security capabilities (Figure 7).

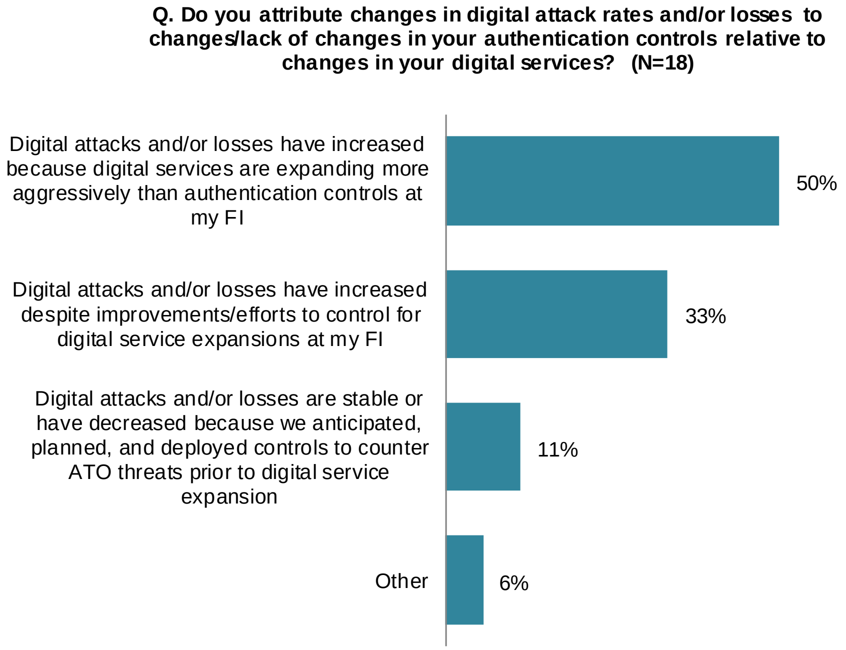
Figure 7: Budget Comparisons—Digital Sales and Service Platforms Versus Digital Fraud Mitigation



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

All of the respondents report that digital sales and service platforms have grown significantly over the past two years and that these expansions have impacted digital fraud attack rates, and most indicate that growth in digital sales and service platforms has had an impact on losses (Figure 8).

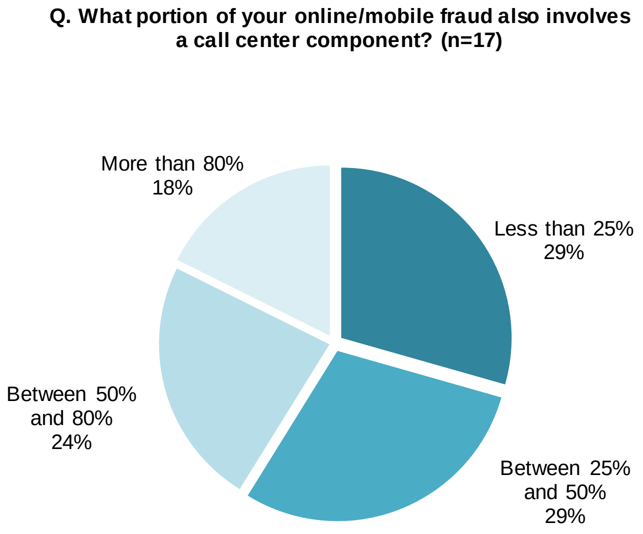
Figure 8: Linkage Between Digital Sales and Service Platform Growth and Digital Fraud



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

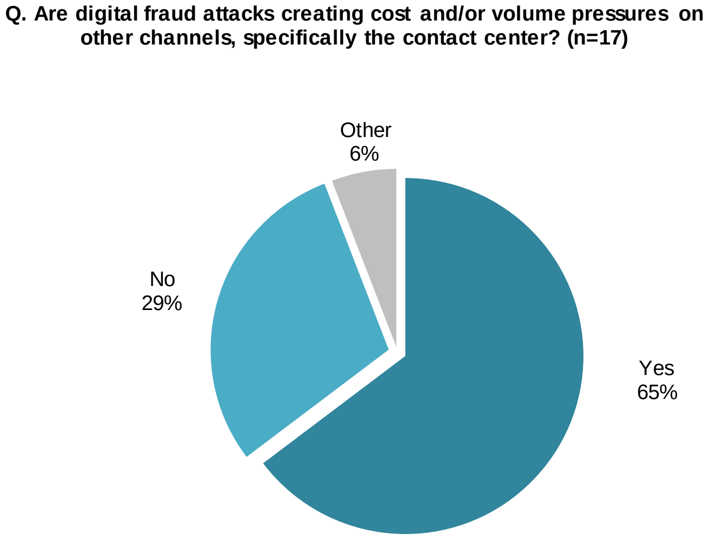
In addition to the general consensus that the expansion of digital sales and service platforms plays a central role in increases in digital fraud activity, there is also consensus that digital fraud activity is a complex ecosystem that impacts (and is impacted by) supporting business units and channels, most notably, the call center. Figure 9 shows the portion of digital fraud that has a call center component, and Figure 10 shows the impact of that fraud.

Figure 9: Digital Fraud With a Call Center Component



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

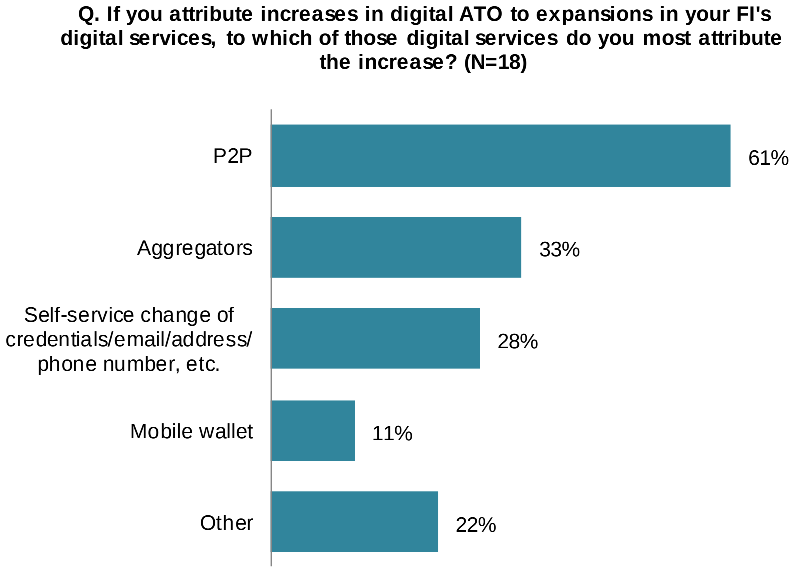
Figure 10: Impact of Digital Fraud on Call Center Volume and Cost



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

In terms of digital fraud trends, interviewed fraud executives expressed a variety of perspectives. Innovations in peer-to-peer (P2P) payment services were among the most often cited digital services behind increases in digital fraud attack rates (Figure 11). It's worth noting, however, that though digital P2P payments account for significant increases in attack rates, most executives (56%) report that they account for 10% or less of their digital fraud losses. It also appears that some banks are still struggling to control for fraud rings that are fond of exploiting authentication vulnerabilities made possible by accommodating aggregators such as Yodlee and Plaid. Finally, it appears that self-service capabilities that enable customers to change addresses, phone numbers, and email addresses are another source of security challenges for fraud executives.

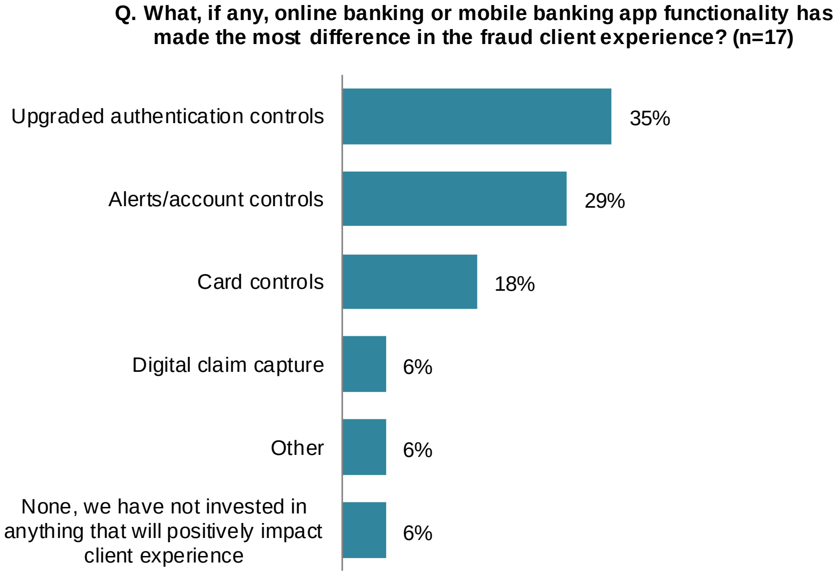
Figure 11: Digital Services Behind Digital Fraud Attack Rate Increases



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

The battle to improve upon digital experiences is one with many fronts, and not all of them are exclusively related to authentication or transaction- and channel-monitoring controls. Many of the fraud executives interviewed report that other, often passive controls also play an important role in making positive impacts on client experience (Figure 12).

Figure 12: Fraud-Related Online and Mobile App Functionalities Impacting Client Experience



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

DIGITAL FRAUD TRENDS

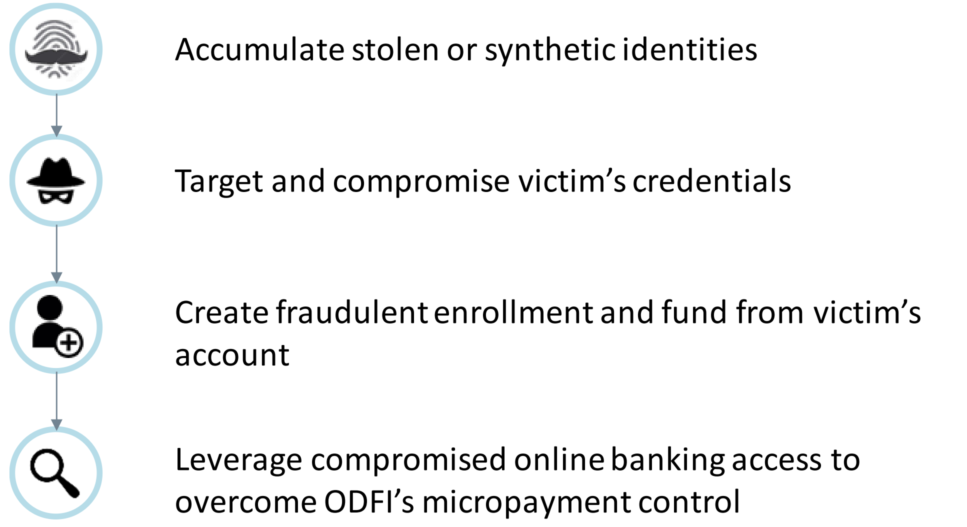
Over the past several years, ATO has evolved and matured in terms of the scale of the problem and the sophistication of tactics.[2] Interviews with fraud executives confirm this trend but also reveal that there is a wide variety of ways in which digital fraud attacks manifest themselves. As was previously illustrated, though there is general consensus that expansions in digital sales and service platforms are a significant driver of digital fraud attack rates, there is less consensus as to how these attack rates manifest themselves and the degree to which they are directly related to expansions in digital sales and service platforms.

ATO AND ONLINE ACH FRAUD

Interviews with fraud executives revealed that there is, indeed, a trend in an ATO scheme consistent with the attack vector that was highlighted in the previous Aite Group report cited (Figure 13), but that it is isolated to a minority (22%) of the FIs that participated in the research. The scheme, likely being driven by one or more criminal rings, involves two FIs. The first FI is home to the source of the stolen funds from a victim's account, usually by way of compromised credentials to their online or mobile profile. The second FI is home to the drop account that, upon opening, is used to initiate an ACH transfer from the victim's compromised account at the first FI. The first FI would, therefore, be the receiving depository financial institution (RDFI) and the second, the bank that initiated the transfer by way of funding the new drop account, would be the originating depository financial institution (ODFI).

[2] See Aite Group's report *Trends in Account Takeover Fraud for 2019 and Beyond*, June 2019.

Figure 13: ACH ATO Scheme



Accumulate stolen or synthetic identities

Target and compromise victim’s credentials

Create fraudulent enrollment and fund from victim’s account

Leverage compromised online banking access to overcome ODFI’s micropayment control

Source: Aite Group

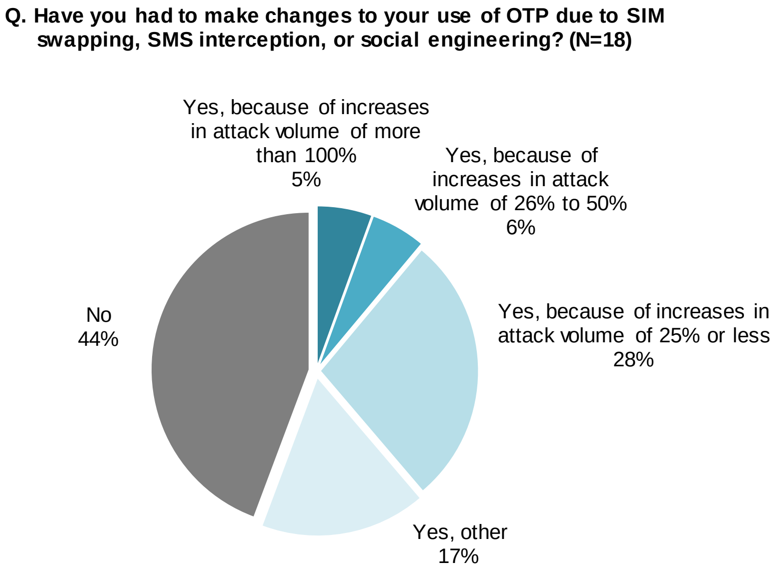
Seven of the 18 participating FIs (22%) report increases in RDFI fraud. Of those seven, one reports an increase in RDFI fraud of between 11% and 25%, two report significant increases of between 25% and 50%, and one reports a substantial increase of more than 50%. The remainder report flat or decreasing rates of RDFI fraud. On the mule side of the scheme, 11 of the 18 FIs (62%) report increases in ODFI fraud. Seven of the 11 report modest increases in ODFI fraud of 10% or less, two report increases of between 11% and 25%, one reports a significant increase of between 25% and 50%, and another one reports a substantial increase of more than 50%. The remainder report either flat or decreasing rates of ODFI fraud.

SIM SWAPPING

Another fraud trend that has impacted some FIs disproportionately is SIM swapping. The scheme involves a fraudster getting possession of the SIM chip that links a mobile phone number to a phone. Once a fraudster has control of the SIM chip, he or she is able to associate a cell phone number with another device that the fraudster controls, thus enabling the interception of text messages and phone calls used by many institutions for multifactor authentication.[3] A little more than half of participating FIs report that SIM swapping attacks are significant enough to motivate them to make changes to their multifactor authentication controls (Figure 14).

[3] “SIM Swap Scams: How to Protect Yourself,” Federal Trade Commission, October 23, 2019, accessed November 16, 2019, https://www.consumer.ftc.gov/blog/2019/10/sim-swap-scams-how-protect-yourself.

Figure 14: The Impact of SIM Swapping



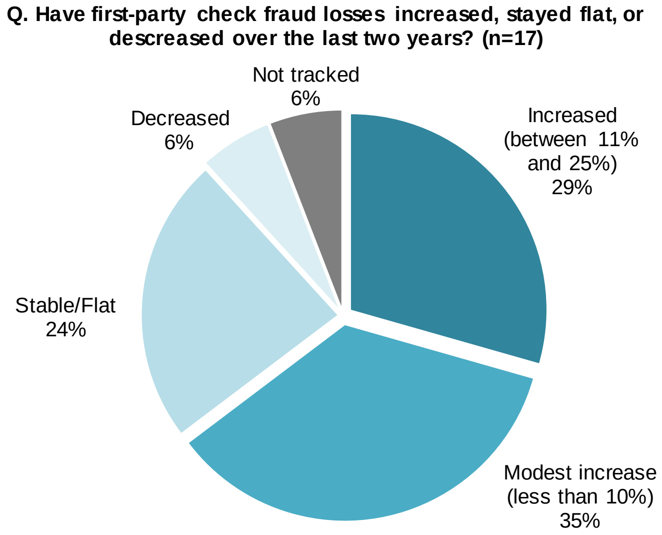
Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

FIRST PARTY CHECK FRAUD

As was reported in the previous report on digital channel fraud mitigation,[4] check fraud has persisted and, for many FIs, has captured (or, in some cases, recaptured) the attention of fraud executives. In fact, of all of the manifestations of digital fraud that were included as part of the interviews for this report, the one that demonstrates consistently widespread impacts is first-party check fraud, with 64% of participating FIs reporting increases. Interestingly, it is the one type of fraud that most fraud executives agree is the most directly related to expansions in digital sales and service platforms (Figure 15).

[4] See Aite Group's report *Digital Channel Fraud Mitigation: Market Trends Influencing FI Strategies*, November 2017.

Figure 15: First-Party Check Fraud Growth and Linkage With Digital Sales and Service Platforms



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

Most fraud executives point to the surplus of stolen and synthetic identities available for use by first-party fraudsters as the most prominent root cause behind these increases. One fraud executive summed up comments by several others by saying "it's a function of the identity data flood." Others also cited mobile deposit capture as the digital service enabler behind its persistence. One fraud executive opined that "as we expand marketing of mobile RDC (remote deposit capture) to our customer base, I expect this to increase." Yet another fraud executive pointed out that pressure to improve funds availability also played a part in the threat's reemergence. Regardless of the root causes, there is general consensus that first-party check fraud is playing an important role in adding to the demand for improvements to identity verification controls as a means of more accurately and effectively screening stolen and synthetic identities from new enrollments.

PRIORITIES

As fraud and digital banking executives struggle to transform their control frameworks in a determined effort to maintain or improve the equilibrium between loss mitigation, client experience, regulatory compliance, and operating efficiency, they've revealed the accumulated demand for fraud controls that are more sophisticated, accurate, and effective than ever before. As the saying goes, necessity is the mother of invention. So the marketplace has responded with a wide variety of innovations that, for those that have prioritized investment in digital security on equal or greater footing with investments in digital sales and service, offer a diverse range of options for building a thoughtful and robust control framework. The timing couldn't be better as the urgency to secure clients from financial crime and to transform the banking experience around a digital-first model is only accelerating as the industry moves toward faster payments and faces an ever-expanding tide of financial crime.

While the variety and diversity of fraud solutions have their benefits, they also bring another significant challenge for fraud executives: how to plot a thoughtful strategic path to transform the control framework without blowing the budget or compounding the complexity and costliness of legacy controls. Table B lists several influential factors in navigating a digital fraud mitigation transformation strategy.

Table B: Challenges and Implications of Formulating a Digital Fraud Mitigation Roadmap

Challenge	Implications
The constant evolution of digital fraud amplifies demand for agility and flexibility among solution platforms.	Choose a platform that offers the right balance of flexibility and breadth of preconfigured modules. Flexibility trumps breadth for most, but some prefer the advantages of "off-the-shelf" functionality.
The nature of digital fraud in traversing channels and business units necessitates greater interoperability among detection systems.	Interoperability is at least as important as capability, especially if/when you need to deploy an orchestration hub. This is particularly true as it applies to integrating horizontally (between channel monitoring systems and transaction monitoring systems) and vertically (between channel monitoring systems and treatment systems, such as those used for stepped-up authentication).
The expectations of clients (and the stakeholders that serve them) require unprecedented accuracy and stealth.	You need to formulate your plan around the notion of bifurcating strategies into those that specialize in finding nonfraud and those that find fraud. The former is at least as important as the latter, but the truth is that they're symbiotic and should work in harmony.

Challenge	Implications
The landscape of solution providers is constantly evolving and shifting.	Choose a partner with a vision that aligns well with your institution's and has the momentum (or promise) that indicates they'll survive the inevitable waves of acquisitions and mergers. If that fails, then it's always a good bet to choose one that plays well with others.
Layered controls are good, and layered (or ensemble) risk models are better.	You can't rely on your data (or your models) alone. The most effective controls are those that are layered, and the most effective models are those that are configured to augment one another. This is particularly true when it comes to having models that are scoped exclusively for the footprint of your operations, augmented by consortium-based models that offer a perspective outside of the footprint of your operations.
Mitigating digital fraud is a journey, not a destination.	Controls that are able to accumulate and make use of an evolving profile centered around multiple features can be far superior to snapshots in time for optimizing accuracy and effectiveness. This is particularly true with regard to monitoring highly complex ecosystems of interactions, such as those associated with ATO or mule activity.

Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

The evolution of digital fraud tactics over the past few years is a reflection of the fraudsters' tendency to seek out vulnerabilities in the control framework that emerge by way of repeated probing and increasingly effective information sharing on the deep, dark web. Therefore, it is an unavoidable fact that vulnerabilities will emerge in the control framework over time. Indeed, with the pace of change in the digital transformation and the rate of expansion of digital sales and service platforms, the emergence of vulnerabilities is accelerating. Couple this with the unfortunate fact that most banks continue to depend (reluctantly, as many will attest) on controls in their framework that they know are increasingly ineffective. No digital fraud mitigation strategy should, therefore, be complete without consideration of a path to compensate for controls in the framework that have outlived their utility.

CONTROLS THAT HAVE OUTLIVED THEIR UTILITY

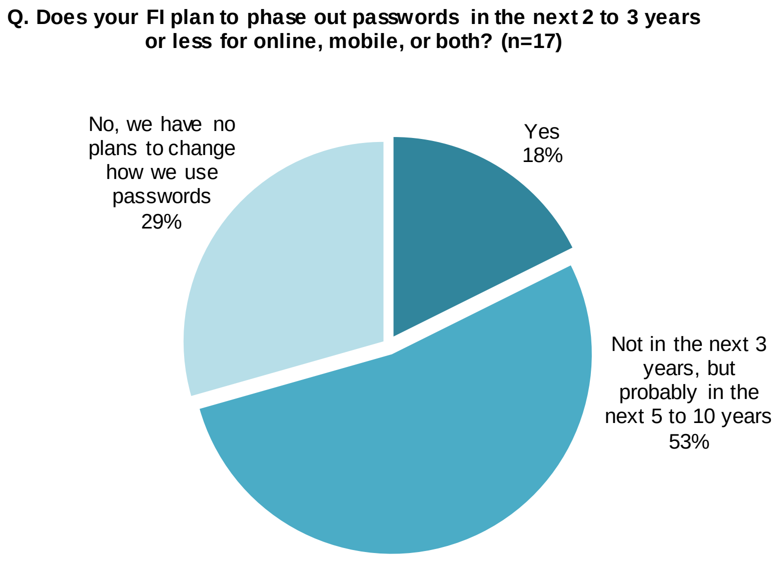
In terms of the effectiveness of security controls, it's hard not to comment on login credentials. According to a study by Google Research, there are an estimated 4.3 billion exposed credentials.[5] The study states that "credential leaks pose a broader risk to the online ecosystem

[5] "Data breaches, phishing or malware? Understanding the risks of stolen credentials", Google Research, November 2017, accessed November 17, 2019, ai.google/research/pubs/pub46437.

due to weak password selection and re-use."[6] Indeed, the tendency of consumers to reuse usernames and passwords is one of the more often cited root causes of ATO attacks among fraud executives. While there are a variety of estimates for the number of credentials that an average consumer maintains, as well as the percentage of credentials that are reused,[7] the conventional wisdom among security professionals is to assume that every credential in the portfolio is compromised. In other words, few if any security professionals believe that the combination of username and password is an effective security countermeasure in isolation.

Among FIs participating in this research, only 29% report that they have no plans to change how they use passwords in the next two to three years. Fifty-three percent of the participating FIs report having plans to replace passwords in the next five to 10 years, and another 18% report having plans to phase out passwords in the next two to three years (Figure 16).

Figure 16: Plans to Phase Out Passwords



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

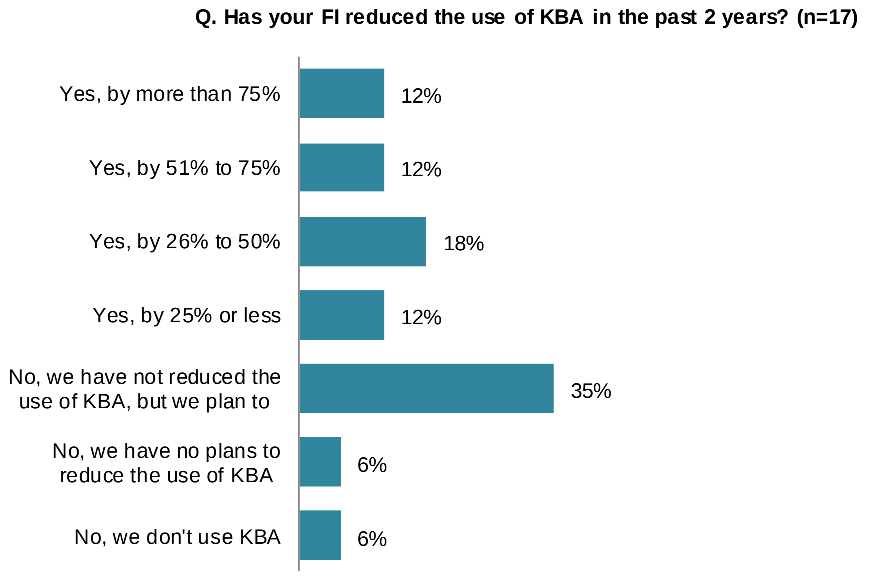
Another often cited control that fraud executives are keen to replace is KBA. Indeed, many fraud executives cite replacing, displacing, or augmenting KBA as one of the primary business case drivers behind digital fraud mitigation transformation initiatives (Figure 17). It is notorious for causing friction in the client experience, is a frequent source of complaints, and, as some fraud executives have claimed anecdotally, is actually more reliable as an indicator of fraud than it is an authentication control. Despite all this, however, there have been relatively few institutions that have made significant progress in replacing KBA. Most have focused their efforts on

[6] Kurt Thomas et al., "Data breaches, phishing or malware? Understanding the risks of stolen credentials," Google Research, November 2017, accessed November 17, 2019, ai.google/research/pubs/pub46437.

[7] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang, "The tangled web of password reuse," In Symposium on Network and Distributed System Security (NDSS), 2014.

displacing it where possible or augmenting it with more effective (and more passive) countermeasures, such as inspection of digital device profiles, mobile network operator (MNO) validation, and behavioral biometric analysis.

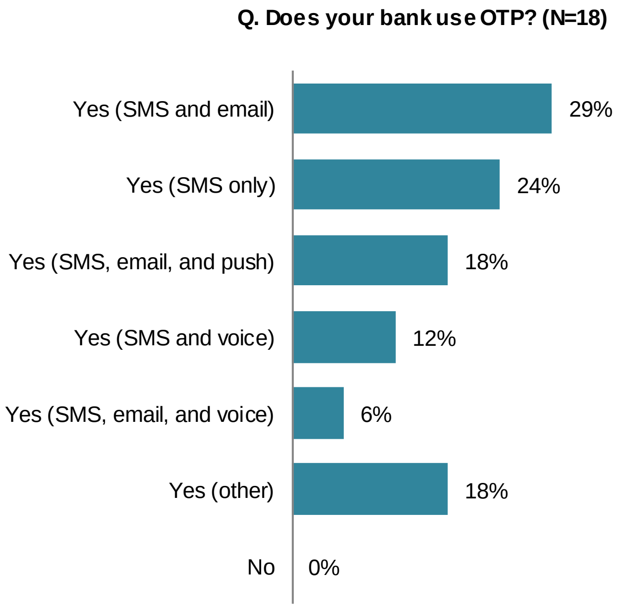
Figure 17: Plans to Phase Out KBA



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

One of the most widely adopted methods for multifactor authentication controls that was originally developed to augment the security of credentials is the use of a one-time passcode (OTP). Every one of the participating FIs reported using OTP (Figure 18), though, as was pointed out earlier, many have been forced to make changes to how they use OTP to compensate for rapidly evolving tactics (e.g., SIM swapping) that seek to defeat the control.

Figure 18: Adoption Patterns of OTP

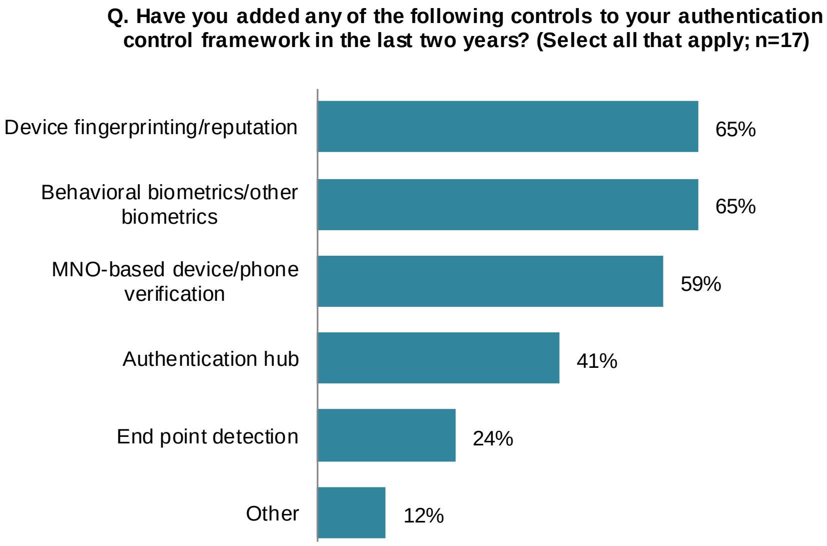


Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

CONTROLS THAT ARE WORKING WELL

Many of the controls that fraud executives report are being used to displace or augment KBA have also been finding favor in boosting the effectiveness of fraud detection, improving false positive rates, and improving client experience. The most widely adopted controls among participating FIs are device profiling/reputation controls, behavioral biometric solutions, and MNO verification solutions (Figure 19).

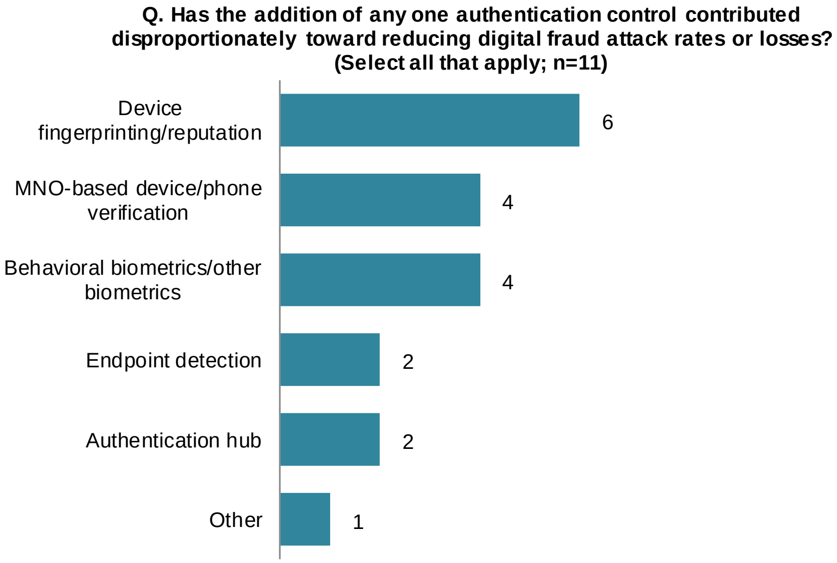
Figure 19: Adoption Patterns of Authentication Controls



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

Among the controls that are cited as having a particularly noticeable impact are behavioral biometrics, device profiling, and MNO verification controls (Figure 20).

Figure 20: Effectiveness of Authentication Controls



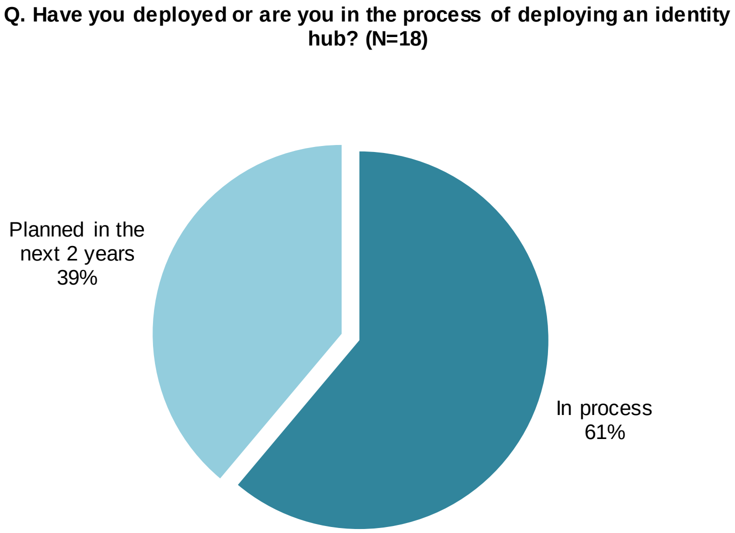
Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

ORCHESTRATION HUBS AND OTHER EMERGING SOLUTIONS

Also benefitting from the intense focus to improve authentication and identity verification controls are orchestration hub vendors. As recent Aite Group research illustrates in greater detail,[8] the increase in demand for these solutions is driven by the proliferation and diversification of authentication and identity verification solutions. As FIs add increasingly varied identity authentication and verification solutions to their control frameworks to address specific gaps, they've done so at the expense of creating siloed domains of control that often overlap with one another, but some have also inadvertently introduced some disruptions in the digital client experience. This is precisely what has driven increased demand for orchestration hubs (Figure 21). The adoption of these orchestration hubs has grown significantly since 2017.

[8] See Aite Group's report *Fraud, Authentication, and Orchestration Hubs: A Path to Greater Agility*, December 2019.

Figure 21: Authentication Hub Adoption



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

Similar strategic objectives of adopting platforms that enable the centralization of policy administration and the optimization of detection and false positive rates are driving forces behind the transaction monitoring marketplace. Vendors that offer a broad spectrum of detection modules in the context of a centralized platform, such as SAS, Actimize, and BAE, continue to enjoy healthy adoption. The challengers to these conventional approaches are the multipurpose analytics platforms that can be molded into multiple point solutions. The market leaders among these solutions, Feedzai, Featurespace, and Simility, have also enjoyed healthy growth rates in terms of adoption. Others, such as IBM's Safer Payments, are beginning to gain traction as well. Vendors that can be deployed for tightly scoped, relatively low-cost deployments as discrete point solutions aimed at resolving a specific use case (e.g., transaction monitoring for wire fraud) but can be later expanded vertically (e.g., expanded to include digital channel signals indicating ATO) or horizontally (e.g., expanded to include transaction and channel monitoring for ACH fraud) are garnering the greatest attention among fraud executives in search of transaction and channel monitoring solutions to fill gaps in their digital fraud control frameworks.

Fraud and digital experience executives are also increasingly on the lookout for solutions that can address well-known and persistent pain points in digital journeys. The most notable of these well-known pain points and the area that has seen a lot of emerging solutions is the card dispute process. Ethoca, a leader in the disputes processing space, has recently launched a new product that has great potential to improve the dispute experience as well as chargeback rates. Ethoca's Eliminator enables card clients to conduct self-service research of card transactions that they do not recognize. Another notable emerging vendor focused on improving client experience specific to the dispute process is Finscend. Finscend's solution is the first commercially available AI-based dispute capture and resolution solution aimed at increasing auto-decision rates by as much as 80%.

CONCLUSION

Many market issues are impacting how FIs are navigating the industry's digital transformation.

Some considerations for fraud executives at FIs:

- Capitalize on the energy to transform digital experiences; partner with stakeholders in the digital and product departments to find opportunities to collaborate in finding (and funding) investments that advance client experience and client security.
- Don't be shy about selling security as a client experience differentiator. The core of the trust relationship between customers and an FI is ensuring that they are protected.
- Develop a robust digital fraud mitigation strategy that emphasizes precisely how to achieve better equilibrium among client experience, fraud loss mitigation, regulatory compliance, and operating efficiency.
- Be diplomatic—but assertive—in making the case for prioritizing investment on equal footing with sales and service platforms as a means of defending against the negative impacts of increased exposure to financial crime.

Some considerations for solution providers:

- Don't underestimate the influence of client experience. Although controlling for financial crime is still a primary objective, it is also true that fraud executives are under exceptionally high pressure to improve elements of client experience.
- Be prepared to illustrate where you fit into the control framework, how well you play with neighboring control solutions, and why and how you complement (or help to optimize or augment) the other solutions in the framework.

RELATED AITE GROUP RESEARCH

Fraud, Authentication, and Orchestration Hubs: A Path to Greater Agility, December 2019.

Trends in Account Takeover Fraud for 2019 and Beyond, June 2019.

Digital Channel Fraud Mitigation: Market Trends Influencing FI Strategies, November 2017.

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

Trace Fooshée
+1.857.406.3515
tfooshee@aitegroup.com

Research Design & Data

Judy Fishman
+1.603.338.6067
jfishman@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