Aite PARTNER. ADVISOR. CATALYST.

Workplace Distancing: Adapting Fraud and AML Operations to COVID-19

APRIL 2020

Julie Conroy

A complimentary copy of this report is provided by:

BioCatch

TABLE OF CONTENTS

LIST OF FIGURES

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

- Aite Group interviewed 13 fraud and anti-money laundering (AML) executives at North American financial institutions (FIs), fintech lenders, and issuing processors from March 31, 2020, to April 8, 2020, to understand how they have adjusted to the new requirements dictated by COVID-19. Interviews also explored the evolving risk vectors as bad actors adjust their tactics to capitalize on COVID-19.
- Fraud and AML operations at financial services firms have not typically consisted of a remote-enabled workforce, nor are most operations centers known for ample space between workers. Therefore, the shift to remote workers and the requirements of social distancing have necessitated a rapid adjustment for firms around the globe.
- The majority of firms interviewed have already migrated 85% or more of their fraud or AML operations to remote work, while two of the FIs interviewed are not nearly as far along.
- Fraudsters appear to be focusing their efforts on application fraud. One fintech lender reports that its front-line tools, which include identity verification and device identity, usually stop between 1.5% and 1.8% of its applications; over the past 60 days, it has seen 5% of applications failing those checks.
- While online and mobile fraud attacks have not yet spiked in the wake of COVID-19, most of the fraud executives interviewed do not believe that this happy state will continue. One large FI executive says that his FI had previously forecast an 8% decrease in fraud in 2020 and has revised that projection to a 10% to 15% increase in fraud for the year, and he says most peer banks have done the same.
- Continuous authentication controls will also be important as person-to-person (P2P) and mobile remote deposit capture (RDC) limits are relaxed. Fraud teams should look at adding low-friction controls covering the P2P journey, such as device identity and behavioral biometrics, regardless of whether they obtain the P2P services via their core provider or are enabling them directly.
- The sudden and dramatic shift to a largely remote workforce promises to change the way business is done after the crisis is over. While financial services fraud and AML operations historically have been primarily conducted in person, firms are finding out firsthand that not only is it feasible to have operations work in a distributed, remote environment, but also that there are benefits in terms of increased productivity, improved morale, and reduced overhead expense.

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

Within a remarkably short period of time, COVID-19 has dramatically altered the way in which the global population works, transacts, and interacts. Social distancing, a term that was not in most people's vocabulary just a few short months ago, is the new norm. Fraud and AML operations functions at financial services firms have not typically consisted of a remote-enabled workforce, nor are most operations centers known for ample space between workers, so the shift to remote workers and the requirements of social distancing have necessitated a rapid adjustment for firms around the globe.

Some organizations were better prepared than others to deal with the implications of the pandemic, but there is a broad recognition that commerce and banking have changed for good, and the pandemic will change the way that organizations work in the future. This Impact Report examines the best practices and lessons learned as financial services firms adjust to the need for a largely remote operations workforce. It also explores the evolving risk vectors as bad actors adjust their tactics to capitalize on the COVID-19 reality.

METHODOLOGY

In this research, sponsored by BioCatch, Aite Group interviewed 13 fraud and AML executives at North American banks, fintech lenders, and issuing processors from March 31, 2020, to April 8, 2020, to understand how they have adjusted to the new social distancing requirements dictated by COVID-19.

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

COVID-19: IMPACT ON FRAUD AND AML

The COVID-19 pandemic rapidly swept across the globe during the first part of 2020. Its highly contagious nature, combined with its high mortality rate, has prompted an emphatic response from governments around the globe as they close schools and nonessential businesses, issue shelter-in-place mandates, and even enforce lockdowns as they seek to contain the new coronavirus.

All these measures have profoundly disrupted commerce, work life, and personal life. Financial services are by no means exempt, although these firms are deemed essential businesses. While debit card spending has held fairly steady, credit card spending is down 20% year over year, according to FIs interviewed for this report. And the impact on lending and capital markets will be profound as a deep recession hits in the aftermath of this disruption. Table A summarizes some of the key market trends that financial services firms and their workforce are contending with, and the subsequent sections elaborate on each of these points.

Table A: Market Trends and Implications

Market trends	Market implications
Bad actors taking advantage	Bad actors thrive on chaos and confusion, and COVID-19 is no exception. Fraudsters are already finding ways to use the pandemic to their advantage, and that will escalate in the weeks and months to come.
Increased remote channel usage	As people are advised to stay at home, most financial services firms are seeing increased use of the online, mobile, and contact center channels.
Shift to a remote workforce	Fraud and AML operations have historically not included a remote workforce. Many financial services firms have had to scramble to facilitate this in the wake of the pandemic.
Internal fraud concerns	Internal fraud is a key concern going into any recession. The combination of a largely remote workforce with access to sensitive data, combined with the expectation of a deep recession post-crisis, has many executives concerned.
Reprioritization of technology investments	Large banks are already forecasting sharp declines to earnings and deep loan losses as a result of the pandemic. Financial services firms will re-evaluate planned technology investments for 2020 and beyond as a result.

Source: Aite Group

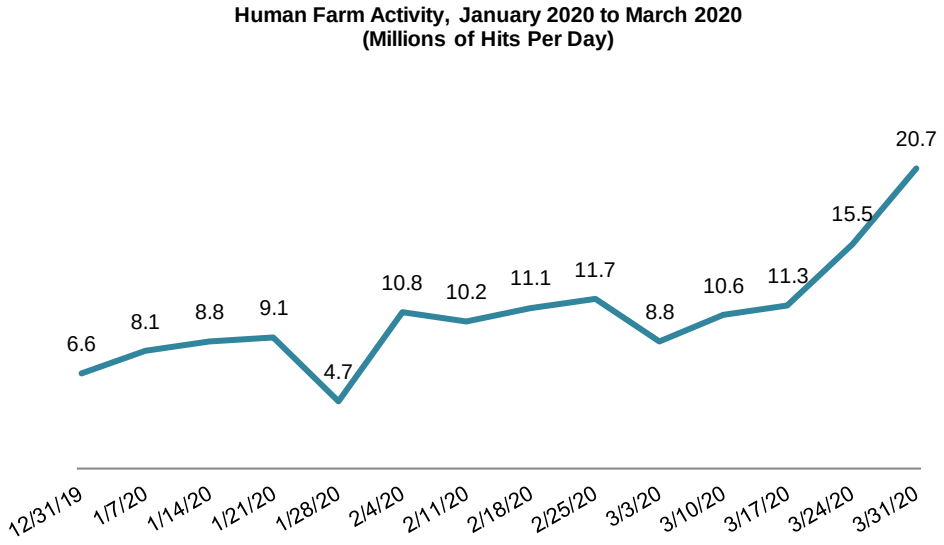
BAD ACTORS TAKING ADVANTAGE

Bad actors thrive in times of confusion, and the COVID-19 pandemic provides fertile ground for organized crime rings to sow their attacks. Thus far, however, fraud attacks have not yet increased across the board to the extent that one might expect. Most of the FIs interviewed say that they have not yet seen a spike in account takeovers, although most have experienced a rise

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 COVID-19-related phishing attacks. Data from Arkose Labs on the activity of human farms[1] during the global pandemic indicates that fraudsters experienced some of the same workforce displacement issues as genuine businesses, but they are rebounding in Q2 2020 (Figure 1).

Figure 1: COVID-19's Impact on Human Farm Activity



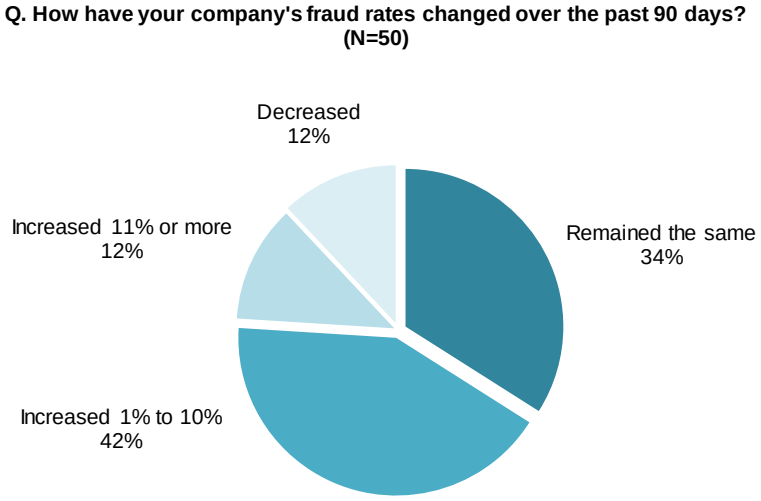
Source: Arkose Labs

Consumers are purchasing many more things online, and most issuers are relaxing their fraud controls somewhat to ensure they do not inconvenience good customers. Even so, card-not-present (CNP) fraud has not yet experienced a sharp spike. The issuers interviewed report CNP fraud increases that are commensurate with the rate of increase in CNP commerce in general over the past 60 days. These results are in line with an April 2020 survey of e-commerce merchants conducted by Kount, in which the majority of merchants report that their CNP fraud rate has either remained the same or only increased between 1% and 10% over the past 90 days (Figure 2).

1. A human farm is a group of low-paid workers hired by organized crime rings to perpetrate attacks using stolen data.

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 2: Change in CNP Fraud Rates, January 2020 to April 2020



Source: Kount survey of 50 e-commerce merchants, April 2020

Fraudsters appear to be focusing their efforts on application fraud. One fintech lender reports that its front-line tools, which include identity verification and device identity, usually stop between 1.5% and 1.8% of its applications. Over the past 60 days, it has seen 5% of applications failing those checks. This fintech lender also does some form of authentication on all applications that make it through the front-line screens, and it is seeing a 30% abandonment rate at that stage, which indicates a threefold increase for both first-party and third-party fraud. Another fintech lender hasn't seen quite such a stark increase, since it has pulled back on a lot of its marketing activities in the wake of the pandemic and in anticipation of a significant resulting recession. This executive said the 25% to 30% increase in post-COVID-19 application fraud that his firm is seeing is "stupid fraud" that is easy to catch, with mocked-up paystubs and falsified tax returns.

While not all FIs interviewed are seeing a similar uptick in application fraud, two of the banks say that they have seen a significant uptick in online deposit account applications that turn out to be the result of mule recruitment scams. This is consistent with industry reports indicating that mule recruitment scams are on the rise as bad actors capitalize on the vast increase in people who are suddenly unemployed and more vulnerable.[2]

CARDHOLDER DISPUTES

As consumers' travel plans have been disrupted, many issuers are seeing significant increases in nonfraud dispute call volume.[3] As consumers transition purchasing behavior to more faceless

2. "Coronavirus Widens the Money Mule Pool," KrebsOnSecurity, March 17, 2020, accessed April 7, 2020, https://krebsonsecurity.com/2020/03/coronavirus-widens-the-money-mule-pool/.

3. See Aite Group's report *The Global Chargeback Landscape: Rapidly Evolving*, November 2018.

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

transactions, an increase in cardholder disputes is to be expected for some time to come. An issuer with a co-brand travel card—unsurprisingly—has seen a twofold increase in dispute volume (mostly related to travel), while an issuing processor that primarily works with smaller FIs has only seen a minor uptick. Another FI that was outsourcing a substantial portion of its dispute workload to offshore facilities saw its domestic dispute operation inundated when the offshore partners were thrust into a mandatory work-from-some scenario, which contravened bank policy that banned offshore operations from working from home.

FRAUD ON THE HORIZON

While online and mobile fraud attacks have not yet spiked, most of the fraud executives interviewed do not believe that this happy state will continue. One large FI had previously forecast an 8% decrease in fraud in 2020, but it has revised that projection to a 10% to 15% increase in fraud for the year and says most of its peer banks have done the same. Table B details the key attack vectors that financial services firms anticipate over the months to come.

Table B: Fraud on the Horizon

Fraud type	Description
Account takeover	Significant increases in phishing activity, combined with the fact that many FIs are relaxing their limits for mobile RDC and P2P transactions, will contribute to an increase in account takeover fraud over the months to come.
Scams and social engineering	Scams and social engineering are already on the rise, aimed at consumers and businesses alike. Financial services firms are bracing for the fallout as consumers and businesses fall prey to everything from mule recruitment scams to business email compromise.
Treasury check fraud	Every FI interviewed is bracing for an onslaught of counterfeit Treasury stimulus checks. Most FIs have underinvested in the area of check fraud for years, so the mitigation of this type of fraud will be painful for many.
Small-business loan fraud	Small-business fraud has always been challenging for banks to manage due to the difficulty of verifying the validity of a new business customer. The chaos surrounding the rollout of the Paycheck Protection Program portion of the U.S. Coronavirus Aid, Relief, and Economic Security (CARES) Act has many fraud executives concerned about the resulting fraud.
Internal fraud	Internal fraud is always a concern during times of recession, but the risk will be further compounded by the sudden transition to a remote workforce.
CNP fraud and disputes	As CNP activity continues to supplant card-present transactions, fraudsters will increase their efforts to mix bad activity in with the good. As unemployment mounts, growing friendly fraud will also be an increasing concern. This will not only impact fraud rates for merchants and issuers but also significantly increase the operational workload for disputes.

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

COMPENSATING CONTROLS

As financial services firms scramble to adjust to the new dynamics, they are (or are not) deploying compensating controls in a variety of ways, as discussed in Table C.

Table C: Compensating Controls

Fraud type	Description
Account takeover	None of the FIs interviewed plan significant immediate changes to their account takeover controls, although one FI says that the increase in digital activity will make it easier for it to obtain 2020 prioritization for incremental protections, such as device identity and behavioral biometrics. One of the FIs interviewed is actually loosening some of its stepped-up authentication controls to make it easier for customers to transact online during this time as well as to reduce the impact on the contact center, but it fully expects increased losses to accompany this business decision.
Mule detection	All but one of the FIs interviewed have some form of mule detection deployed. One FI indicates that its strategies focus on social media recruitment and remote deposit capture, and it is successfully averting a significant amount of the activity and potential losses.
Card fraud strategies	Most of the changes FIs are making to card fraud strategies are incremental (e.g., increasing tolerances for grocery and CNP purchases and tightening around travel purchases and restaurants) now that people aren't going out and about. One of the FIs interviewed says that it has switched from a monthly view of fraud patterns in its report to a daily view, since transactional activity is changing so rapidly. Most FIs are anticipating the typical recessionary uptick in first-party fraud and are tuning strategies accordingly.
P2P fraud	While many FIs are increasing P2P limits, one FI has addressed the incremental risk associated with P2P by cross-training its AML staff to help work the potential overflow that could result from a spike in P2P fraud. Continuous authentication controls will also be important as P2P limits are relaxed. Fraud teams should look at adding low-friction controls covering the P2P journey, such as device identity and behavioral biometrics, regardless of whether they obtain the P2P services via their core provider or are enabling them directly.[4]
Treasury checks	While check fraud detection has been underinvested in for years, the best practice is to combine imaging technology, consortium data, and manual review.

Source: Aite Group

INCREASED REMOTE CHANNEL USAGE

While most North American FIs have not closed their branches entirely, most have seen a significant reduction in branch traffic, which ranged from 15% to 30% among interviewees. Contact center volume has increased substantially as a result—the consistent figure that emerged from virtually all interviews indicates contact centers are contending with a 40%

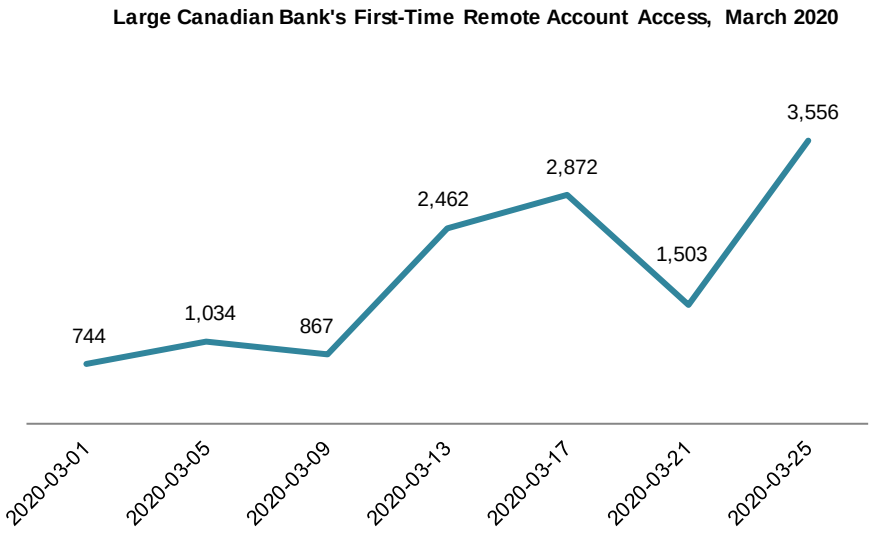
4. See Aite Group's report *Best Practices to Thwart Fraud in Real-Time Payments*, October 2019.

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

increase in call volume. Much of this spike materialized just as firms were transitioning to a remote work environment, so in the words of one FI fraud executive, "It got pretty hairy."

While not all of the firms interviewed have seen a big uptick in online and mobile channel usage, the majority of interviewees have. One FI reports a 250% increase in digital channel usage in a single week in late March in the wake of the COVID-19 shelter-in-place orders, and a number of others report incremental usage of digital channels as well as services such as remote deposit capture and P2P. This trend is substantiated by BioCatch data that shows a strong uptick in customers who remotely accessed their account for the first time as COVID-19 fears and shelter-in-place orders accelerated during March 2020 (Figure 3).

Figure 3: Increase in First-Time Remote Account Access



Source: BioCatch

SHIFT TO A REMOTE WORKFORCE

Many firms' business continuity plans (BCPs) contemplate the need to transition to a largely remote workforce, but executing on a plan of this magnitude often entails a few surprises and bumps in the road. Table D details the extent to which each of the firms interviewed has transitioned its fraud or AML operations team to a remote workforce, and the extent to which the affected team previously had remote capabilities.

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

Table D: Progress Toward Remote Enablement

Firm type/size (in US$)	Number of employees and composition	Percentage remote-enabled as of April 8, 2020	Prior remote enablement of affected workforce
FI with more than $200 billion in assets	1,250 financial crime staff	98%	25%
FI with more than $200 billion in assets	280 fraud analysts and investigators	6%	0%
FI with more than $200 billion in assets	250 AML analysts and investigators	100%	60%
FI with $100 billion to $199 billion in assets	80 fraud analysts and investigators	90%	Less than 10%
FI with $100 billion to $199 billion in assets	100 deposit fraud analysts and investigators	20%	0%
FI with $100 billion to $199 billion in assets	300 fraud analysts and investigators	90%	0%
FI with $100 billion to $199 billion in assets	1,000 fraud analysts, investigators, and contact center staff	More than 85%	Less than 10%
FI with $20 billion to $99 billion in assets	150 fraud analysts and investigators	More than 85%	Less than 10%
FI with $20 billion to $99 billion in assets	200 fraud and AML analysts and investigators	100%	40%
FI with $20 billion to $99 billion in assets	22 card fraud operations employees and investigators	98%	50%
Fintech lender	250 people, including fraud, AML, call center, and collections	100%	Less than 10%
Fintech lender	Eight fraud analysts and investigators	100%	100%
Issuing processor	540 people, including fraud, disputes, call center, and collections employees	85%	Less than 10%

Source: Aite Group interviews with 13 fraud and AML executives, March to April 2020

The majority of firms interviewed have already migrated 85% or more of their fraud or AML operations to remote work, while two of the FIs interviewed are not nearly as far along. One of these FIs expected to get to 30% to 40% remote by April 10, 2020, but it does not plan to have more of its fraud operation to a remote environment unless the COVID-19 crisis significantly

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

escalates. This FI is seeing 20% absenteeism in its fraud operation as workers stay home due to lack of childcare, illness, or fear of COVID-19 exposure. Another of the FIs interviewed has no current plans to have any of its fraud operation work remotely. It has rearranged its operations center to allow six feet of distance between employees. This FI was seeing 70% absenteeism in late March, but it provided financial incentives to operations staff to come in and is now down to an average of 20% absenteeism.

For the time being, most of the firms interviewed do not to expect to get to a full 100% of their operations workforce working remotely. Some workers do not have internet at home, so for them, remote work is not an option. And the realities of fraud and dispute operations require having people on-site to receive the mail and faxes, and scan customer documents into the system. However, with a substantial portion of most operations teams now working remotely, it is easy to space the onsite people to ensure they can observe social distancing requirements. In the case of one FI, a building that previously housed 1,500 employees now only has 20 people physically there on a day-to-day basis. Another firm has taken the additional step of segregating on-site employees in different parts of the building with separate air circulation units and different points of entry to further ensure separation.

As the scope and severity of COVID-19 in North America became apparent in early March, many of the firms interviewed underwent an intense BCP execution period. Table E shares some of the executives' observations about the transition at their firm.

Table E: Observations About the Transition Effort

Firm type/size	Quote
FI with more than US$200 billion in assets	"We were never set up for remote capabilities. We were in the process of looking at this when this hit and accelerated what we were doing. Today we are at 6% remote, we expect to be at 30% to 40% remote by April 10. We will cycle employees between remote and on-site week by week. If things get worse, then we can go 100% remote."
FI with US$100 billion to US$199 billion in assets	"We had to get ramped up quickly—we did a good job, but fraud ops had to stand in line behind customer-facing staff. Contact center and lending ops had priority."
Fintech lender	"On March 9, IT started aggregating hardware, we started doing test runs department by department. We got through all departments by March 12. By March 13 we were officially 95% remote, and by March 20, we were 100% remote."
Issuing processor	"We finished the transition in a record time frame and with zero degradation in service levels and responsiveness. A lot of planning made this so successful."

Source: Aite Group

COLLABORATION

Fighting financial crime is often a collaborative endeavor—in a fraud or AML operations center, valuable ad hoc verbal communication often takes place over the cube walls among analysts and investigators. Many of the firms interviewed have deployed technology or increased their use of existing deployments to help facilitate communication in the virtual environment.

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

Microsoft Teams is in use by a number of the FIs interviewed. The platform enables workplace chat, video meetings, and file collaboration, among other things. One of the banks rolled it out in late January 2020 and said that its use significantly increased as the operation shifted to a remote environment in March 2020. Another of the firms that uses Microsoft Teams launched a new case management system the first week of April. Although 100% of this firm's staff is now remote, it said the launch came off without a hitch and gives part of the credit to the easy collaboration facilitated by the Microsoft Teams platform. Jabber and Slack are additional collaboration tools cited by FIs interviewed.

BEST PRACTICES

Best practices that helped facilitate an easier transition to a remote operations workforce include the following:

- **Preexisting remote workforce:** While self-evident, the extent to which a firm's operation was previously remote-enabled is a key determinant in how easy it is to transition to a remote environment. One of the fintech lenders introduced remote work to its operation a year ago, when changes to its business processes dictated the need for people to start working night shifts. One hundred percent of its fraud operation was remote-enabled at that time, which made the COVID-19 transition seamless. On the other end of the size spectrum, one of the large banks interviewed for this research introduced the remote work option for its financial crime operations staff three years ago to improve both morale and productivity. The success of this initiative spread to other operational units, so for this FI, the COVID-19 shift has been relatively seamless compared to some of its peer banks. And one of the large processors indicates that after it got over the initial hump of increased call volume at the same time that it was transitioning its workforce to remote work, it has now seen its call center's speed-to-answer time decrease in a remote workforce environment.

- **Advanced planning:** For the majority of financial services firms that did not have a substantial portion of their operations team working remotely prior to the crisis, it's not as easy as just buying some laptops and sending everyone home. The firms also need to have the appropriate licensing and hardware to enable remote access servers, VPNs, and the requisite information security tools to monitor data usage and access. While many had this conceived theoretically as part of their BCP, the reality of execution can occasionally have some unexpected challenges.

- **Send the hardware home:** A hallmark of fraud and AML operation centers is that most desks have two to three monitors to increase productivity. Some of the firms interviewed encouraged their staff to take their monitors home, although one executive at an FI that did not says that even though his staff feels the lack, the numbers show that his newly remote workforce is still operating more productively due to the elimination of commute time, fewer meetings, and in some cases fewer distractions (although the distraction factor is by no means universal, since many workers are contending with young children at home).

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

- **Practice makes perfect:** One FI saw the writing on the wall and performed a drill in early March. This bank outfitted all employees with the equipment to work from home and had everyone work remotely. During the first day of the drill, there were VPN capacity issues, and the bank had to pull a few people to service customers, but this exercise helped work out the kinks for the shelter-in-place orders that came later in March.

- **Emphasize work/life balance:** A challenge for all remote workers is maintaining a balance between work and personal life. This challenge is compounded as people are thrust into remote work for the first time while dealing with the stress of the pandemic and having children home from school and day care. One bank interviewed has seen a slight decrease to productivity since it transitioned to a remote workforce, but that was by design. This bank added two weeks to its employees' accrued paid time off and is encouraging staff to take time as needed to care for family members. Another FI executive says that his team has become more productive as they have transitioned to remote work, but some of that is the result of employees working long hours and late nights. When this takes place, managers are actively encouraging those workers to take comp time. In this executive's words: "This virus will be a marathon, not a sprint, so we need to keep people fresh."

- **Enable self-service.** All firms interviewed saw a sharp spike in call volume at the outset of the crisis. One firm analyzed its call center data and identified that requests for payment deferral represented a substantial portion of the inbound volume. This firm enabled self-service capabilities in its interactive voice response (IVR) and website to facilitate payment deferrals and saw call volume quickly decrease as a result.

- **Scale back time demands on customer-facing business partners:** An AML executive at a large global bank indicated that his group has provided relief to the bank's business units where possible. His department has stopped its AML requests for information (RFIs) to the lines of business so they can focus on customer-facing priorities. Whereas the lines of business previously had 60 days to resolve Know Your Customer discrepancies, the deadline has now been pushed to 90 days, and they are currently contemplating extending that time frame to 120 days. Engagements in which the AML team tests business-line policies and procedures have stopped for the duration of the crisis. The only area in which the RFIs remain in place at this FI is related to the bank's regulators. It is currently in the process of its annual Office of the Comptroller of the Currency (OCC) exam. Unlike the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)[5], the OCC has not yet provided any statements saying it will provide regulatory relief related to the crisis, so the AML unit is still sending exam-related RFIs to its business partners. On the other hand, an AML executive at another large FI states that as of yet, his FI does not feel that it has the ability to give any reprieves to business partners. This FI does say

5. Jacqueline D. Shinfield, "FINTRAC Issues COVID-19 Guidance to Reporting Entities," Blakes, March 27, 2020, accessed April 16, 2020, https://www.blakes.com/insights/bulletins/2020/fintrac-issues-covid-19-guidance-to-reporting-enti.

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

that since regulatory examiners also have shelter-from-home requirements, the pace of response has slowed a bit, because communication via email rather than in person facilitates a more methodical response cadence.

- **Keep documenting:** As financial services firms adjust their risk controls, whether it's from an AML, credit risk, or fraud perspective, documentation of these changes remains important. As one executive interviewed says, "While regulators say they will be forgiving during these times, we know there will be a reckoning, so we are very carefully documenting everything."

LESSONS LEARNED

Even for the most prepared financial services firms, this transition has not entirely been smooth sailing. Some of the headwinds that interviewees report include the following:

- **Supplier issues:** Many banks had to buy a large number of laptops to equip workers to work remotely. Concurrent with this surge in demand, Dell's supply chain was adversely impacted when multiple Dell partner facilities and fulfillment centers were hit by the severe tornados in Nashville in late February 2020. Many banks had to scramble and procure laptops from other vendors. A couple of banks indicated that, absent the ability to get more laptops, they packed up employee desktops and sent them home, and dispatched IT people to the employees' houses to set them up properly.

- **Capacity issues:** Multiple firms report technology hiccups (understandably) as a result of the abrupt shift to a remote workforce. One large bank increased remote access server capabilities as part of its migration plan, but even so, the executive interviewed says that around 3:30 pm ET most days all of a sudden the servers seize up—Outlook and large file downloads from the shared server freeze due to volume overloads. Another bank reports periodic issues with the phone system's capacity, which result in poor call clarity or delayed calls, and sometimes staff are abruptly kicked out of the system. This FI executive says that there is some sort of a minor technology issue that needs to be addressed daily.

- **Adjustment to family concerns:** The large FI that only has 6% of its workforce remote-enabled is struggling with absenteeism—on average, 20% of its operations staff is not coming to work. This is driven by a combination of workers with no childcare now that schools and day cares are closed, workers who are sick, and those who are just afraid to come to work. Those FIs that have transitioned to a largely remote workforce are also having to be flexible, as many employees confront the challenge of working from home while also acting as full-time parents and teachers to their kids confined to the house.

- **New type of management:** It's not just employees who are having to make adjustments to working remotely—managers are having to learn on the fly as well. Managing a large operations staff remotely requires that managers develop new practices and habits to keep tabs on the team and workload, making more use of dashboards and reporting as well as technologies that can facilitate workload

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

balancing and monitoring. Some executives interviewed have initiated daily morning calls to discuss key activities, identify potential issues, and prioritize work. These calls can help keep the team apprised of ongoing developments, account for absences and spikes of work, and often reduce the need for ad hoc meetings throughout the day.

INTERNAL FRAUD CONCERNS

Concern over accidental data leakage and internal fraud has historically been a significant obstacle that prevented many financial services firms from embracing a remote operations workforce.[6] This concern is not just from an internal fraud and reputational risk perspective; there are also compliance drivers, as FIs need to meet the regulators' reasonability expectations with regard to data security controls.

Internal fraud and data protection are key concerns for many of the executives interviewed, although the extent of that worry varies widely. Some executives point out that while there can be greater controls to address internal fraud in a bank operations center, many of those same controls can be extended into a home office environment. The biggest issues mentioned by respondents that are largely out of the FI's control in a home office include the ability of staff to write down or photograph sensitive customer information, or the ability of family members or roommates sharing the living space to do so. Devices connected to the internet of things, such as Amazon's Alexa, smart baby monitors, and home security systems, are also exposure points; a number of the executives interviewed state that they issue periodic communications to remind employees to turn those devices off in their workspace. And, of course, home router security is a critical requirement for all remote workers.

Best practices among participants to control for internal fraud among remote workers include the following:

- **Inventory personally identifiable information (PII) visible in each system.** In many operations centers, the primary data leakage prevention control is a clean-room environment maintained by the various system vendors. One of the banks interviewed has inventoried the PII visible in each system, and if there are functions in which the clean room does not work in a remote environment, the FI will work to mask PII that the end user doesn't need to see.

- **Perform behavioral analysis.** Many of the firms interviewed have systems in place to monitor the degree to which PII is being accessed by employees, then compare that to behaviors across their peer group to identify anomalous activity.

- **Maintain visibility.** Visibility into worker activity is a key control (along with clear communication to the workforce that the visibility exists). One executive interviewed said that his system enables him to see everything that his employees are doing systematically. Others indicate that they can track what operations staff are looking at via thin clients on the employees' machines, can prevent employees

6. See Aite Group's report *Employee Fraud: Anticipate a Resurgence*, January 2020.

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

from printing to home printers, and can see if they take something from work email and send to their personal email.

- **Value staff and compensation maturity.** One of the firms interviewed said that the majority of its remote fraud team is quite mature in both tenure and compensation, which, in theory, should lower the risk that those employees would be tempted to risk their position for an opportunistic crime.

REPRIORITIZATION OF TECHNOLOGY INVESTMENTS

As many banks shift a large portion of their workforce to remote work and are confronting a likely economic downturn to follow this crisis, some are reprioritizing their technology investments. For a few of the FIs interviewed, this means that many technology projects in the pipeline are somewhat in limbo. Some of those projects that were "nice-to-have" versus "must-have" will be reprioritized or even canceled. In other cases, the increased emphasis that the crisis is placing on digital channels is resulting in the prioritization of projects to better secure digital channels, such as device identity and behavioral biometrics. As one executive observed, in the post-crisis recession, there may be less budget to work with, which will drive the need to further leverage technology and automation for better detection and greater operational efficiency.

FUTURE STATE

One point that nearly all the executives interviewed for this report concurred on was the fact that this sudden and dramatic shift to a largely remote workforce promises to change the way business is done after the crisis is over. While financial services fraud and AML operations historically have been primarily conducted in person, firms are finding out firsthand that not only is it feasible to have operations work in a distributed, remote environment but also that there are benefits in terms of increased productivity, improved morale, and reduced overhead expense. One executive sums up the consensus sentiment when he says, "Our bank will definitely take a look at this going forward. Do we really need all this expensive floor space? I could see this leading to a significant work-from-home shift." Another executive echoes the sentiment when he says, "On the other side of this, there will be a cultural change to how people work." And a third says, "We were already exploring the opportunity for top performers to work remotely, so this has been an accelerated pilot."

Another aspect of business as usual that at least one FI interviewed expects to revisit post-crisis is the reliance on offshore workers. This bank has a policy against offshore workers working from home. When shelter-in-place orders came, and the offshore operations effectively went away, the bank's domestic workforce was immediately overwhelmed.

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

CONCLUSION

Unfortunately, the pandemic promises to be a global reality for quite some time. Here are recommendations for financial services firms as they adjust their operations to the new normal:

- **Prepare for fraud attacks on a variety of fronts.** Fraudsters are currently focusing on application fraud attacks, along with a plethora of phishing and mule recruitment efforts. However, expect digital channel fraud and CNP attacks to mount, as bad actors capitalize on relaxed risk controls and a wealth of available data to fuel their attacks. Tools that can effectively assess the risk associated with a new or returning client in a largely frictionless manner are essential. The control framework will also require that firms have the ability to take action, quickly respond to emergent fraud trends, and introduce the appropriate action in an automated fashion.

- **Enable your workforce for the marathon, not the sprint.** A remote or socially distanced workforce is likely to be the new reality for some time to come. Ensure that your technology is equipped to support this and that your firm's culture is supportive of this new normal.

- **Enable (and protect) self-service.** As clients accelerate their migration to digital channels, the importance of easy and secure self-service is more important than ever. Financial services firms need to not only deploy critical functions into self-service channels but also be able to enable the mechanisms to secure these capabilities.

- **Continuous assurance is important as transaction and velocity limits are relaxed.** Fraud and security teams need to look at adding low-friction controls covering the journey leading to the P2P flow if it's serviced by a P2P provider, or covering also the enrollment and payment flow if it's serviced by the banks themselves. Recommended controls in both options are device identity and behavioral biometrics.

- **Revisit your BCP.** Scientists have been predicting this pandemic for years, but many of the firms interviewed were not prepared for a shelter-in-place requirement of this magnitude. Examine your BCP plan and incorporate the lessons learned.

- **Look to the future.** The previously normal state of working will not be the new normal once this pandemic is behind us. Be open to new ways to deploy, empower, and motivate your workforce.

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

COVID-19: Challenges and Opportunities in Financial Services, March 2020.

Employee Fraud: Anticipate a Resurgence, January 2020.

Best Practices to Thwart Fraud in Real-Time Payments, October 2019.

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

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

CONTACT

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

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
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 BIOCATCH

BioCatch pioneered behavioral biometrics, which analyzes an online user's physical and cognitive digital behavior to protect users and their data. Today, customers around the globe leverage BioCatch's unique approach and insights to more effectively fight fraud, drive digital transformation, and accelerate business growth. With nearly a decade of data, more than 50 patents and unparalleled experience analyzing online behavior, BioCatch is a leader in behavioral biometrics. For more information, please visit www.biocatch.com.

CONTACT

For more information on BioCatch products and services, please contact sales@biocatch.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