Aite PARTNER. ADVISOR. CATALYST.

Beating the Bad Guys: Safe and Secure Transactions in the IVR

OCTOBER 2020

Prepared for:

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
INTRODUCTION 4
METHODOLOGY 4
CONTACT CENTER FRAUD 5
FRAUD IN THE IVR 7
PINDROP IVR PROTECT 12
CONCLUSION 14
ABOUT PINDROP 15
CONTACT 15
ABOUT AITE GROUP 16
AUTHOR INFORMATION 16
CONTACT 16

LIST OF FIGURES

FIGURE 1: CONTACT CENTER FRAUD LOSS TREND 5
FIGURE 2: LIKELIHOOD OF SUBSTANTIVE CHANGE IN CONTACT CENTERS 6
FIGURE 3: LOSS LEVELS COMPARED TO INVESTMENT PLANS 6
FIGURE 4: AREAS GETTING FUNDED FOR TECHNOLOGY INVESTMENTS 7
FIGURE 5: EVIDENCE OF FRAUDULENT ACTIVITY IN IVR 8
FIGURE 6: IVR MONITORING 9
FIGURE 7: FRAUD CASES LINKED TO IVR 9
FIGURE 8: PLANS TO MONITOR IVRS 10
FIGURE 9: TOP BUSINESS CASE DRIVERS 11
FIGURE 10: BUSINESS CASE DRIVERS BASED ON FRAUD ALINKAGE TO IVR 11
FIGURE 11: IVR FRAUD CASE STUDY 13

EXECUTIVE SUMMARY

Beating the Bad Guys: Safe and Secure Transactions in the IVR, commissioned by Pindrop and produced by Aite Group, describes the current market environment of contact center fraud in financial institution (FI) contact centers, fraud activity in interactive voice response (IVR), and FIs' technology investment plans to combat such fraud. In addition, it describes the new capabilities of Pindrop Protect and the value of detecting suspicious activity in the IVR.

Key takeaways from the study include the following:

- Thirty-six percent of FIs have seen contact center fraud losses rise in 2020 compared to two years prior.
- Sixty-four percent of FIs are likely to invest in contact center fraud prevention technology in the next two years.
- Identity verification/application fraud controls, contact center identity authentication controls, and digital identity authentication controls are the top three areas getting technology funding.
- Thirty-five percent of FIs plan to invest in monitoring IVR activity in the next two years.
- Improving operational efficiency and the customer experience are the top two business case drivers for contact center fraud technology investments.
- Pindrop Protect IVR case study shows a lapse time of 30 to 60 days for the bulk of fraud to manifest after detection in the IVR.
- Detection of suspicious IVR activity can provide additional fraud savings above and beyond what is detected by other fraud prevention systems in place.

INTRODUCTION

Contact centers are often the least-protected delivery channel in FIs and are frequently the source of cross-channel fraud; typically, the fraud manifests as account takeovers. Many fraud executives lack good insight into contact center activity and often have even less insight into IVR activity. Fraudsters use data gleaned from data breaches and other sources (including reconnaissance work in the IVR) to successfully impersonate customers, leading to the aforementioned account takeover fraud. Adopting a technology solution that can detect suspicious activity in incoming calls going to agents can help prevent account takeover fraud; extending the protection to the IVR enables the FI to better protect impacted accounts and further reduce fraud losses. Taking advantage of these fraud reduction benefits, in addition to reducing the average handle time of calls and improving the customer experience, results in a huge win-win.

This white paper will be of interest to fraud executives as well as contact center management and customer experience executives. The paper discusses the challenges associated with understanding fraud activity in contact centers, the importance of upgrading authentication methods to improve customer experience, and the benefit of reducing the average handle time of calls to improve operational efficiency. Using a robust contact center solution can help an FI reap all these benefits and continue to keep pace as fraudsters evolve their attacks.

METHODOLOGY

Aite Group conducted research using an online survey from September to October 2020 to better understand contact center fraud loss trends as well as gain insight into IVR suspicious activity and technology investment plans. The data reflects input from 47 financial fraud executives from 30 financial services firms. With one exception (Thailand), these financial institutions are in North America, while the nature of the participating fintech firm allows it to cover a wider geographic area.

In addition to the online research, telephone briefings were held with Pindrop to understand the Protect IVR product and the recent pilots that have been conducted with a number of clients.

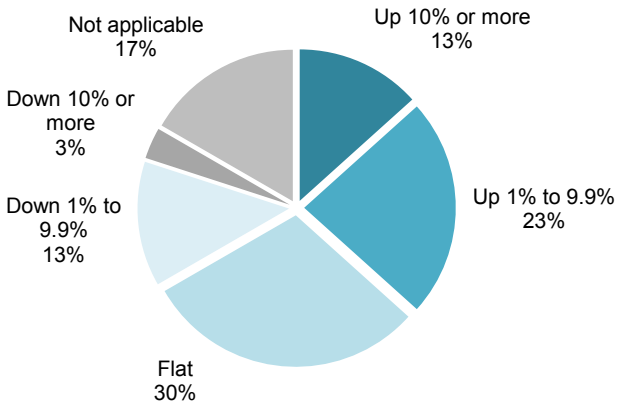
The data reported in this paper are directional in nature.

CONTACT CENTER FRAUD

Of all the types of fraud, contact-center-enabled fraud is often the most difficult to quantify. In many cases, the amount of the loss doesn't reach the dollar threshold each FI establishes to perform root cause analysis of the loss. Because contact center fraud frequently manifests as cross-channel fraud, the loss is often associated with the channel the loss occurred in rather than the contact center that enabled it. For example, if a customer impersonator is successful and is able to get online credentials reset on an account, then transfers funds out of the account, the loss is likely to be classified as online or mobile fraud (whichever is used to sign in to the account and initiate the funds transfer). The FI is often unaware of the link back to the contact center, and the fraud losses associated with the contact center may only include unauthorized transfers performed in that channel. However, even in light of the fact that contact center losses are often understated, 36% of FI executives recognize that they are growing (Figure 1).

Figure 1: Contact Center Fraud Loss Trend

Q. Please indicate the trend associated with contact center, comparing 2020 losses to losses two years ago. (n=30)

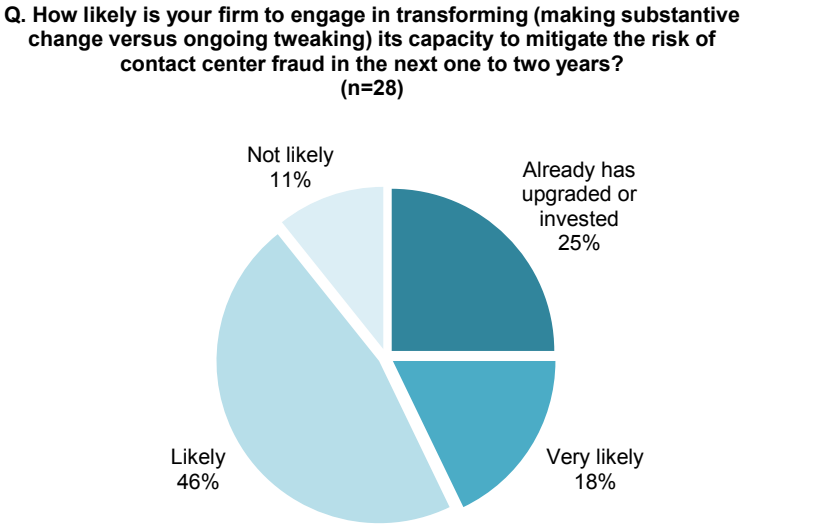


Source: Aite Group survey of 47 financial fraud executives, September to October 2020

Financial crime executives realize that criminals seek the weakest link in an institution to exploit; they also understand that as other FIs implement solutions to protect their contact centers, unprotected contact centers are more likely to be targeted. Eventually, the unprotected contact centers become more vulnerable to attacks by organized criminal rings seeking the easiest way to steal funds.

Only one-quarter of FIs indicate they have already transformed the environment to better protect their contact centers, while an additional 64% indicate they are likely or very likely to do so in the next one to two years (Figure 2).

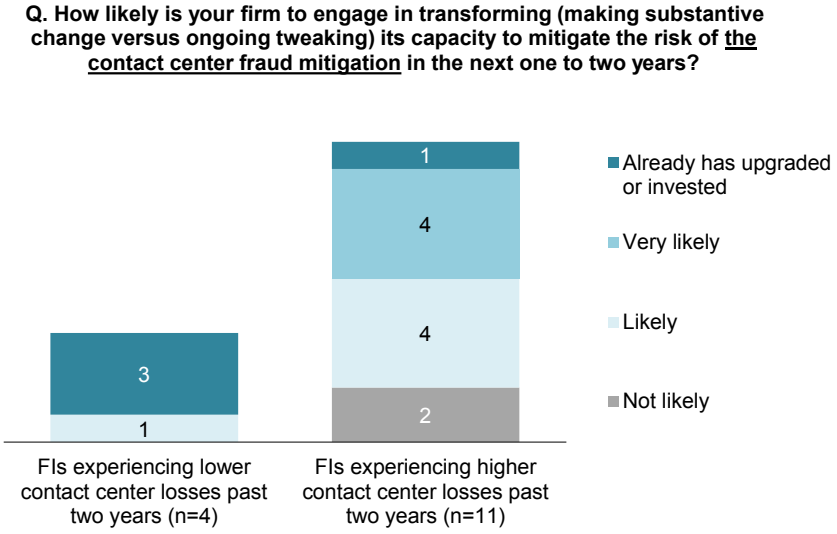
Figure 2: Likelihood of Substantive Change in Contact Centers



Source: Aite Group survey of 47 financial fraud executives, September to October 2020

To better understand the current status of fraud in contact centers, Aite Group compared FIs' plans to invest to reduce contact center losses. In FIs whose losses were lower in 2020 than two years prior, three of the four FIs have already invested in technology to protect contact centers or have upgraded technology. In FIs experiencing higher contact center losses in 2020, eight of the 11 are at least likely to invest to better protect the environment (Figure 3). When contact center losses are clearly understood, it is easier to make a business case to address them.

Figure 3: Loss Levels Compared to Investment Plans

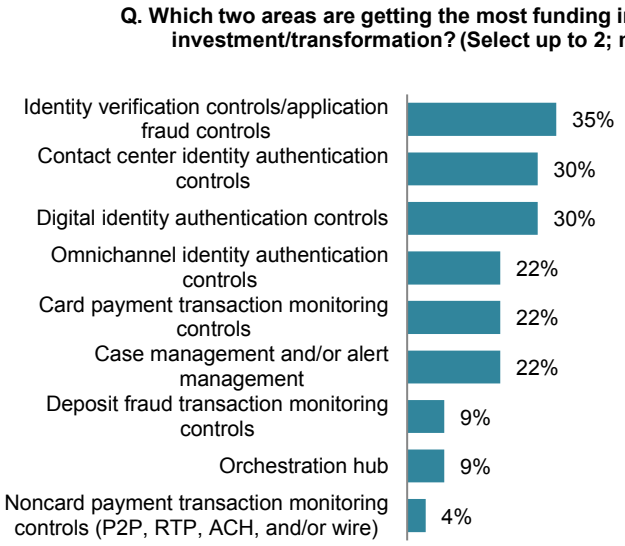


Source: Aite Group survey of 47 financial fraud executives, September to October 2020

FIs have many needs for technology investments or upgrades, given that organized criminal rings are constantly evolving attack methods. Each individual FI can only make so many technology investments annually; similarly, they can only manage a limited number of new technology implementation projects during one year, given the demand on IT resources. Many technology needs exist, particularly in light of the number of new remote channel users as a result of the pandemic. Still, contact centers clearly need protection provided by technology investments.

On a varied list of technology investment opportunities, contact centers tied for second place in terms of gaining investment funding to improve identity authentication controls. In fourth place are omnichannel identity authentication controls, another area in which fraud prevention can be strengthened using data from contact centers that is often used to successfully impersonate customers in other channels (Figure 4). As stated earlier, much contact-center-enabled fraud manifests as account takeovers in other channels. A contact center solution that captures data harvested from IVRs can assist in combating cross-channel fraud.

Figure 4: Areas Getting Funded for Technology Investments



Source: Aite Group survey of 47 financial fraud executives, September to October 2020

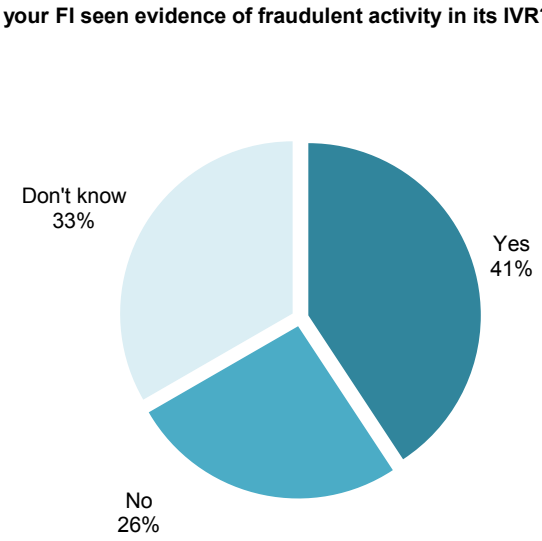
FRAUD IN THE IVR

While many FIs have little insight into the fraud originating in their contact centers, even fewer have insight into how fraudsters are using their own IVRs against them. Fraud executives know organized fraud rings often automate their fraud attacks, using bots to bring down their online banking websites or to perform credential stuffing attacks. They may not realize these same methods are used to help determine such things as where people hold bank accounts or which FI issuer owns the stolen card data they hold. IVRs can be used to test data and determine where it is recognized—in other words, where valued customers do business and what their account looks like. This enables fraudsters to more successfully target their future attacks, making the attacks more lucrative. Here are four ways IVRs are most often used by fraudsters:

- **Information mining and leakage:** Fraudsters gather, test, and augment the data they have from data breaches and other sources to plan and refine future attacks. As an example, they may target accounts with the highest balances or open-to-buy amounts.
- **Account surveillance:** Fraudsters can use IVR data to determine accounts' available balances so they can prioritize which accounts to attack and maximize the amount stolen (by timing attacks with payroll deposit dates, etc.).
- **PINs and passwords:** Fraudsters may use the IVR to change a PIN or password, making it easier to take over a specific account.
- **Cross-channel fraud:** Fraudsters can use information obtained from the IVR to more easily pass authentication in other channels, such as online, in contact centers, or in branches.

Forty-one percent of FIs have seen evidence of fraudulent activity occurring in IVRs, while 26% have seen no evidence of fraud to date. The others (33%) don't know if such activity has occurred in the IVR (Figure 5).

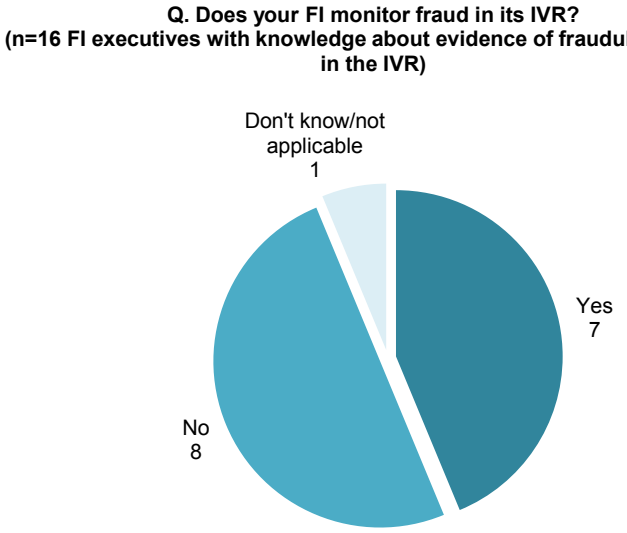
Figure 5: Evidence of Fraudulent Activity in IVR



Source: Aite Group survey of 27 financial services firms, September to October 2020

Among the FIs that have seen evidence of fraudulent activity in the IVR, less than half are monitoring activity in the IVR (Figure 6). Those that are monitoring are using a solution from a technology provider, a solution developed in-house, manual review, or some combination of these methods.

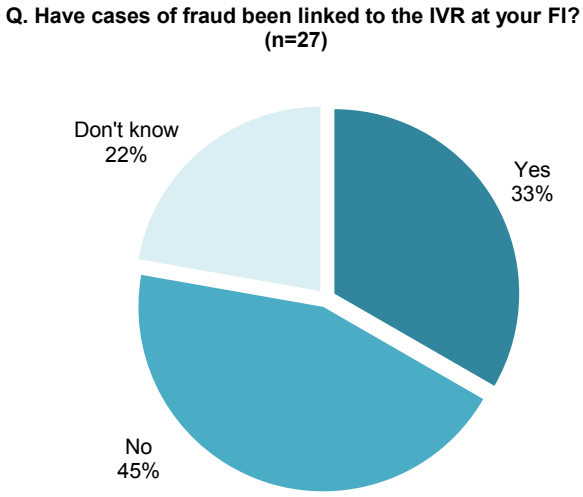
Figure 6: IVR Monitoring



Source: Aite Group survey of 27 financial services firms, September to October 2020

One-third of FIs have linked fraud cases to their IVRs; 45% have not made such linkages, and 22% don't know whether any fraud cases are linked to the IVR (Figure 7). It would be very difficult for FIs with little to no insight into IVR activity to link fraud cases to the IVR.

Figure 7: Fraud Cases Linked to IVR

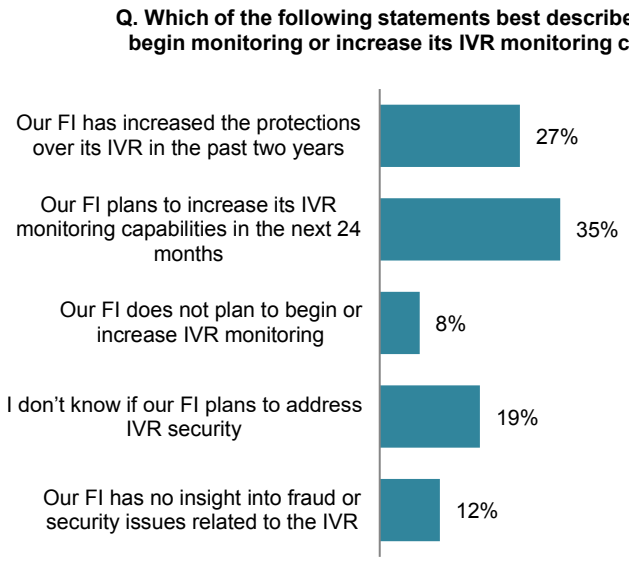


Source: Aite Group survey of 27 financial services firms, September to October 2020

Over a third of FIs (35%) plan to increase their IVR monitoring capabilities within the next 24 months. This 35% is in addition to the 27% that have already increased the protections over the

IVR in the past two years (Figure 8). Only 8% of FIs surveyed do not plan to increase IVR fraud monitoring.

Figure 8: Plans to Monitor IVRs



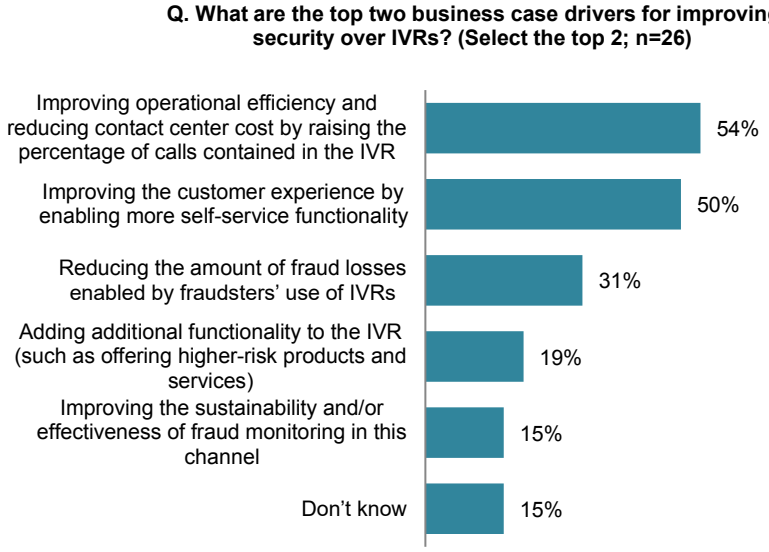
Source: Aite Group survey of 27 financial services firms, September to October 2020

For FIs interested in improving the security of IVRs, the top three most important business case components to justify the technology investment are as follows:

- Improving operational efficiency by containing more calls in the IVR
- Improving the customer experience by offering more self-service options
- Reducing fraud losses enabled by fraudsters' use of the IVR

Improving the customer experience has been and continues to be a high priority for many FIs. In contact centers, the use of knowledge-based authentication questions and one-time passwords introduces a lot of friction and forces customers to go through lengthy processes before their calls can get their needs met. In many cases, the process may add two to three minutes to the call, making it far more costly. Being able to authenticate callers without using these vulnerable processes improves the customer experience and reduces the average handle time of a call (Figure 9).

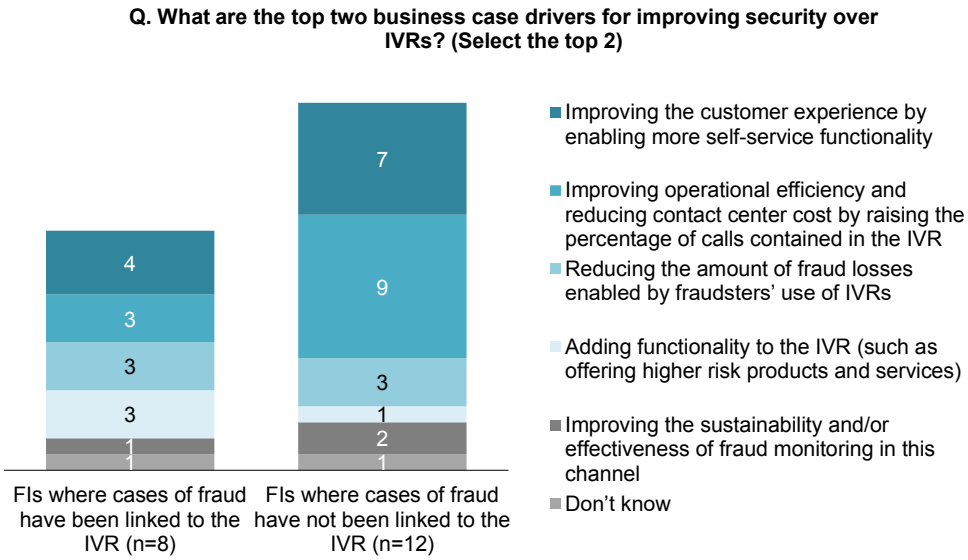
Figure 9: Top Business Case Drivers



Source: Aite Group survey of 27 financial services firms, September to October 2020

An additional benefit of being able to reliably authenticate known customers in the IVR is the ability to offer additional products and services through that channel, further improving operational efficiency. Reducing fraud losses as a business case element appears to be of greater importance in those FIs that have been able to link fraud cases to the IVR (Figure 10). Having the visibility into how fraudsters leverage the IVR to commit cross-channel fraud provides a strong driver to invest in contact center security.

Figure 10: Business Case Drivers Based on Fraud Linkage to IVR



Source: Aite Group survey of 27 financial services firms, September to October 2020

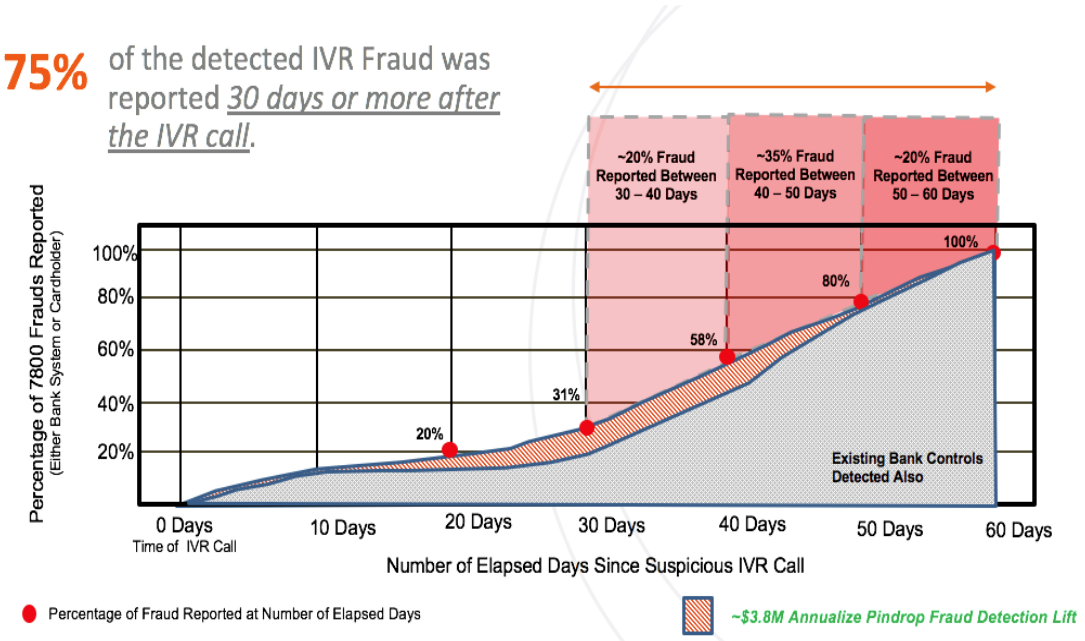
PINDROP IVR PROTECT

Pindrop's Protect product uses a great deal of data to determine the risk score of each incoming call answered by an agent. Pindrop is well known for "Phoneprinting"—associating customers' specific devices to their accounts and phone numbers so that the devices can be identified quickly during incoming calls. Metadata—a wide range of other factors collected on each incoming call that is used to help with risk scoring the call—is also used. Pindrop offers voice and behavioral biometrics, and uses a variety of other data elements that can be incorporated into the call risk scoring and authentication. In addition, Pindrop has created a consortium to enable its FI customers to share data that helps everyone better detect fraudulent activity. One FI fraud executive recently commented that the FI gets a lot of benefit from the consortium and just wants to see more FIs participating; obviously, the more participants, the more sharing, to everyone's mutual benefit. Providing feedback to Pindrop (easily accomplished via APIs or other methods integrated during product implementation) is essential so that machine learning models constantly improve.

In addition to calls going to agents, Pindrop Security has been studying the behavior of fraudsters in IVRs for some time, seeking to understand the activities performed in the IVR and the end results sought by the bad guys. Pindrop has refined its Protect product to incorporate monitoring IVR activity based on all its learnings, and it offers it to existing as well as new clients that want to fully protect their contact centers. While not all IVRs have introduced the use of voice yet, Pindrop uses all of the other available data points to detect suspicious activity. This includes carrier metadata, data on behavior, device intelligence, caller ID validity, and spoof detection, which identify call risk. Furthermore, Pindrop is now introducing Pindrop Trace, which provides an advanced account risk assessment based on artificial intelligence and graph analytics. Pindrop Trace is a network-level view of the complex relationships between multiple accounts and calls across time and helps uncover hard-to-detect fraudsters who operate in rings and use complex fraud tactics. Trace also provides an advance notice of future fraud events by detecting high-risk activities, connections, and behaviors that may otherwise go undetected with simple risk-based models. As the use of voice becomes more common and is expanded in IVRs, it will enable enhanced detection capability. Protect IVR is offered via cloud as well as an on-premises installation. Pindrop offers a lab tenant in which user acceptance testing can be performed prior to using new capabilities in production.

Prior to offering Protect IVR broadly, Pindrop performed pilots with several customers to measure the impact of adding IVR monitoring. Figure 11 summarizes the results of one case study. Clearly, fraudsters are gathering data and planning their attacks based on data gathered in the IVR. This case study demonstrated that several weeks often elapse between data gathering in the IVR and the attacks that are conducted on targeted accounts. The majority of fraud related to the IVR was reported at least 30 days following the detection of suspicious calls in the IVR. One of the most important findings during this pilot was that detecting and acting on suspicious IVR activity prevented over US$3 million in fraud (annualized) over and above what was detected by other fraud prevention systems in use at the piloting company. This data is used to protect accounts in an omnichannel environment, since the fraud is most often attempted in delivery channels other than the contact center. Of course, results will vary from pilot to pilot, but these types of results exemplify the potential value of IVR monitoring with Pindrop Protect IVR.

Figure 11: IVR Fraud Case Study



Source: Pindrop Security

CONCLUSION

FIs should consider all aspects of the contact centers, looking for opportunities to improve the operation. Contact center technology solutions can improve many aspects of the operation simultaneously. Executives at FIs should take the following actions:

- **Consider opportunities to improve the customer experience in the contact centers by reducing the use of knowledge-based authentication questions and one-time passwords.** Both methods are vulnerable to being defeated by fraudsters, and both introduce a great deal of friction into the customer experience. Using passive methods of authentication enables customers' needs to be met much more quickly and makes the interaction more pleasant. Passive methods also reduce the average handle time of a call dramatically; by reducing the average handle time of the majority of calls, operational efficiency can be improved significantly.
- **Investigate the root cause of fraud losses in order to make sound technology investments.** Since contact-center-enabled fraud often manifests in other delivery channels, it can easily be misunderstood, misclassified, and understated. Perform as much root cause analysis on account takeover losses as possible, investigating to understand whether there is a contact center interaction or IVR activity that enabled the fraud to occur, regardless of which delivery channel was ultimately used to steal the funds.
- **Monitor activity in the IVR to determine how fraudsters are using it to plan and conduct attacks against your customers' accounts.** IVR activity, correctly studied and used, can help you better protect targeted accounts across all delivery channels.
- **Consider a robust contact center solution that can passively authenticate customers using the IVR.** This will allow securely offering new products and services via the IVR, further reducing costs and improving customer service.
- **Take advantage of consortium opportunities to share data among FIs.** This enables all to benefit from others' fraud experiences.

ABOUT PINDROP

Pindrop solutions are leading the way to the future of voice by establishing the standard for security, identity, and trust for every voice interaction. Pindrop solutions protect some of the biggest banks, insurers, and retailers in the world using patented technology that extracts an unrivaled amount of intelligence from every call encountered. Pindrop solutions help detect fraudsters and authenticate callers, reducing fraud and operational costs, while improving customer experience and protecting brand reputation. Pindrop solutions have been implemented in eight of the top 10 U.S. banks and five of the top seven U.S. life insurers. Additionally, 70% of Pindrop's U.S. customers are Fortune 500 companies.

Pindrop is constantly improving and expanding its product line to meet its customers' needs, laser focused on an increasingly customer-experience-centric world. Pindrop's contact center solutions leverage patented technologies, such as Phoneprinting, Toneprinting, Deep Voice, and proprietary risk engines powered by an industry-leading consortium of fraudsters' data to provide an end-to-end and continuous view of every call from a risk and caller authentication perspective.

Pindrop Passport

Pindrop's Passport solution is a multifactor authentication solution that reduces friction for genuine callers by providing passive authentication prior to connection with call center agents, thus significantly reducing average handle times, decreasing costs, enhancing self-service, and hardening vulnerable call centers by eliminating absolute dependence on knowledge-based authentication.

Pindrop Protect

Pindrop's Protect solution is a multifactor anti-fraud detection solution that helps fraud teams to stop fraud in real-time, predict future fraudulent activity, reduce fraud-related costs, improve efficiency and review rates, and defend the contact center from attack. Unlike other solutions, the Protect solution works from IVR to agent, identifying which calls are risky and which accounts are likely to be attacked as well as which adjacent channels are vulnerable to fraud.

Pindrop's Solutions on Amazon Connect

Pindrop's solutions are available natively on Amazon Connect, enabling contact centers to provide an enhanced customer experience during caller authentication while fighting the rising threat of fraud. Amazon is a trademark of Amazon Services LLC and/or its affiliates.

CONTACT

For more information, please contact Pindrop:

pindrop.com | 866.245.4045 | info@pindrop.com

Twitter | Facebook | LinkedIn

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

Research Design & Data:

Judy Fishman
+1.617.338.6067
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