SECURING THE CONTACT CENTER

DECEMBER 2019

Licensed by:

NUANCE

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

ABOUT JAVELIN:	Javelin Strategy & Research is a research-based advisory firm that helps clients make informed decisions in the digital financial world. It provides strategic insights for financial institutions, government, payments companies, merchants, fintechs and technology providers.
AUDIENCE:	Banks, credit unions, small-business payments, payment service providers, payment networks, and merchants
AUTHORS:	Krista Tedder, Director Fraud Management
CONTRIBUTORS:	Jacob Jegher, President James Lee, Analyst, Digital Banking Crystal Mendoza, Production Manager
EDITOR:	Craig Lancaster

OVERVIEW

Walk through a contact center and you will hear violations of security and privacy in the name of servicing the consumer. As we collected information on location at multiple contact centers, it was readily apparent that contact center security needs a makeover. Large and small financial institutions, processors, merchants, and technology companies were assessed to determine best-in-class standards of contact center security; however, a best-in-class solution was not found. Every contact center had significant vulnerabilities that were identifiable by speaking with agents and operational staff, and by listening to consumer conversations.

From the information gathered in the art of the conversation to the data validated to verify the caller, all rely on the weakest link of security—humans. With a sophisticated toolkit, criminals can spoof calls, artfully gather data, and take over accounts without the representative being aware that the true person is not on the call. Or worse yet, when account and transaction information is modified for someone perceived to be a close relation (spouse, child, or executive assistant), the account is at risk.

Contact centers are generally not where security professionals reside, yet it is the front door for criminal activity. A maze of outsourced providers—attributable to necessity or design—provides minimal infrastructure for the building of protective barriers in the contact center itself. No one group is given the funding or the staff required to solve the challenges that contact centers bring. The only way to stop the trend of account takeover is through a collaborative approach and by deploying new security technology.

PRIMARY QUESTIONS

- What types of fraud occur when contact centers are not secure?
- How are contact centers secured when there are multiple entry points?
- What technology capability is needed to minimize the threats faced by financial institutions and merchants?

EXECUTIVE SUMMARY

The complexity of evolving consumer contact channels creates new entry points for criminals to take over accounts. Inbound calls remain the highest rate of contact (35%), but growing use of digital channels (22%) and non-traditional channels (social media, SMS, email, etc.) means the threats are evolving to incorporate newer channels.

Account takeover is the leading threat to accounts—card and non-card—than before the U.S. EMV migration. Account takeover has risen from $1.5 billion in 2015 to $4 billion in 2018. Without upgrading technology standards at contact points, the number will continue to rise in 2019-2020.

Taking over an account starts with one action but cascades to the modification of several components of the consumer's identity to obtain access to funds. Physical address (25%) and email address (21%) changes, along with adding an authorized user to an account (23%), are leading activities that lead to account takeover.

Companies are most likely to make changes to minimize threats when a new risk is identified versus being prompted by an existing problem that has been plaguing the industry. Among executives asked, new risks (54%) and regulatory changes (47%) were leading drivers to addressing security incidents. Account takeover is not new and is not raised to the highest risk levels.

Criminal sophistication in both technology and organizational capabilities builds a wave of attacks that companies are not prepared for. Tools to manipulate, influence, and deceive can easily bypass existing authentication protocols and lead to the takeover of accounts.

Financial institutions and merchants are siloed into multiple platforms and providers, which creates hurdles in deploying technology and processes across all business lines. Because not all channels are protected in the same way, criminals will find the most vulnerable point to exploit. If one area has strong consumer authentication but another channel has limited resources, criminals will obtain information where they can first, then work through the channel that has the most funds available to steal.

Organizations generally have fraud detection as a separate unit focused on transactional activity, leaving the contact center open for criminals to attack. High-risk calls are being handled by customer service representatives who do not have a background in understanding fraud.

Disputes can fall outside of the Reg E and Reg Z requirements but still need to be addressed holistically. Channel-specific processes have moved dispute management to processes versus understanding the root cause of the problem. A large-scale account takeover attack could affect numerous consumers, but due to channel-based resolution processes, the criminals are successful in attacking multiple accounts.

RECOMMENDATIONS

Expand contact center objectives to involve more than customer care metrics and include a focus on securing sensitive information. Technology upgrades for authentication provide different metrics that can monitor success and failure rates, fraud potential, and vulnerability assessments.

Create three new organizational responsibilities, either internal or with a third-party provider, to manage high-risk activities. Inbound fraud detection, high-risk calls, and dispute management need to be addressed to protect the organization from large-scale threats of account takeover.

Define inbound fraud detection as protecting the contact center from high-risk contact and not the receiving of callbacks from consumers who received a potential fraud alert. Segmenting high-risk calls to move them away from agents not skilled in fraud will provide a proactive approach to reducing account takeover versus the handling of cases after losses have already occurred.

Deploy technology that minimizes the risk that an agent will assist the criminal in taking over an account. Not all technology is new—screen pops with authenticated data, push notifications confirming identity, and VoIP calls initiated in mobile sessions will reduce the likelihood of a criminal attempting to take over an account being serviced by an untrained fraud team.

Add layers of security through artificial intelligence and advanced analytics to minimize the risk of account takeover. Phone printing technologies to minimize spoofing, monitoring of behavior anomalies, natural language understanding across channels, and continuous authentication provide benefits to minimize fraud loss and negative impacts to consumers whose accounts are taken over.

Expanding the definition of dispute to be more than a chargeback but also inclusive of scams that are meant to perpetrate a crime will be a first step in understanding the scale of the problem. Investigating incidents that are not tracked as fraud in the payment channel but where the customer is a victim of a scam will help identify large fraud rings gathering data to eventually take over accounts.

Improve resolution of dispute claims using next-best-action analytics across channels to ensure consistent responses and the ability to navigate the complex web of rights and responsibilities. Reduce the likelihood of missing fraud events and providing misinformation across channels to quickly understand the scenario and identify the best resolution or method of assisting.

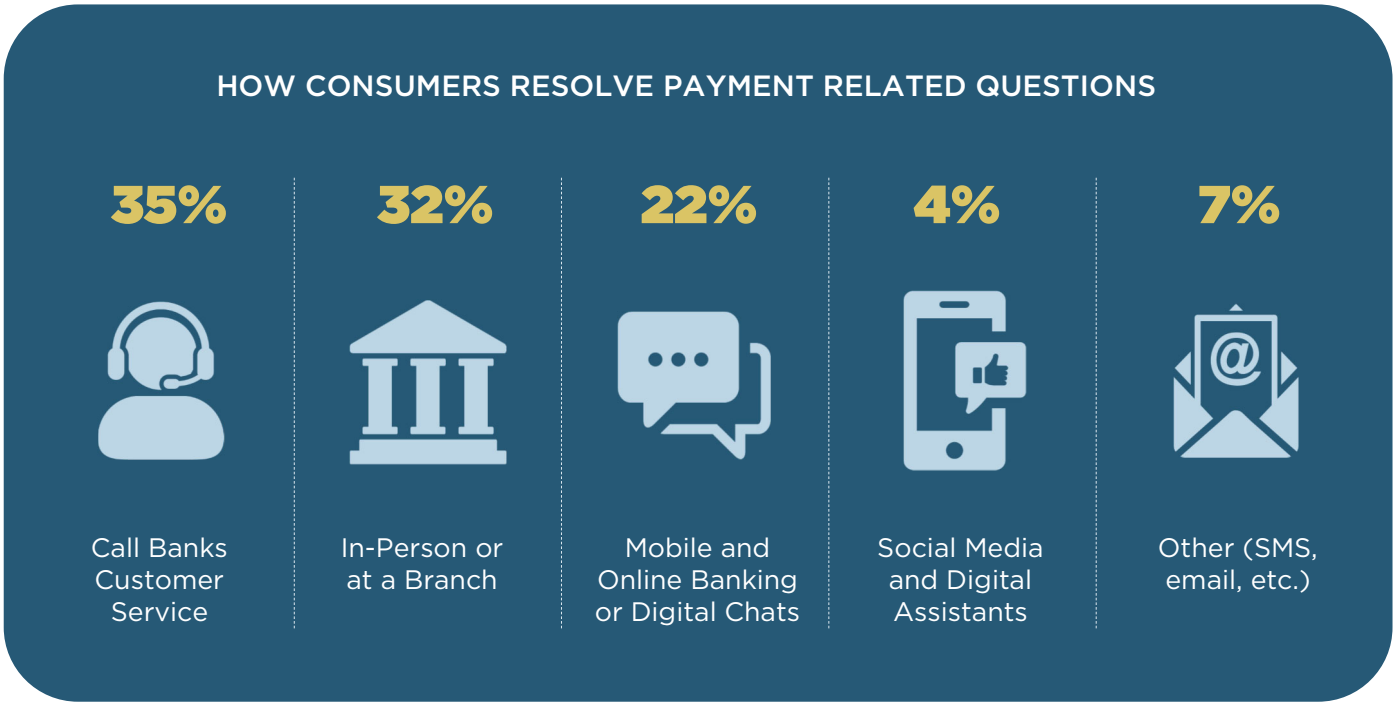
Extend dispute case management tools outside of the payment card channels and leverage a dispute investigation tool that can look holistically at the challenge. Using API and file delivery integration from payment platforms can provide a cross-channel access to disputes to track, enable investigations, and support the recovery of funds.

Deploy mobile adaptive training programs that the agent and consumer can participate in together to allow for detailed question-and-answer sessions to minimize future risks. Educating employees and consumers through shared experiences and guided interactions will help in reducing instances of account takeover after a consumer is a victim of a scam.

THINK LIKE A CRIMINAL, NOT AS A CUSTOMER

To get a question answered, consumers no longer need to call. They can utilize self-service, virtual assistants, online and mobile banking chats, social media messaging, and live agent via voice access through devices (both inbound and outbound contact). The primary method of resolving questions continues to be the contact center for consumers (35%), with over one-third of questions being addressed. However, not having security mechanisms and operational protocols in place for lower-volume requests can add operational risk to the organization. Waiting until an incident occurs to add security is downright dangerous.

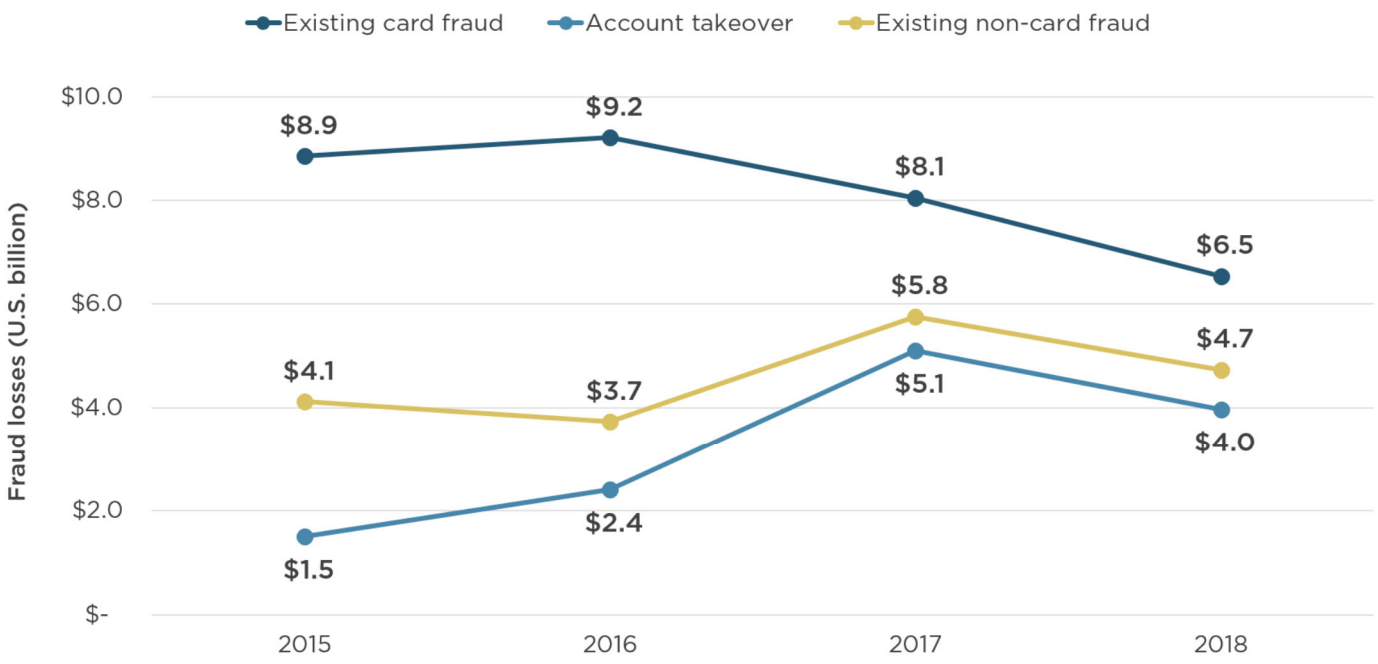
Mixed with the growing risks of social engineering and account takeover, trusting who is in communication with the company becomes a crucial component of every interaction. The movement of fraud from the existing card channel to new-account fraud and account takeover heightens the need for advanced security at the contact point. Fraud losses in the United States reached $15.2 billion in 2018, with account takeover rising at the highest rate from $1.5 billion in 2015 to $4 billion in 2018. Without key security contact center infrastructure to prevent account takeover, the losses will mount.



Source: Javelin Strategy & Research, 2019

New-Account Fraud Grew by $400 Million from 2017 to 2018

Figure 1. New-Account Fraud (NAF) Incidence and Losses (2013-2018)



Source: Javelin Strategy & Research, 2019

Most financial institutions and payment service providers focus consumer authentication within the interactive voice response (IVR) technology or basic validation when consumers reach an analyst. Asking basic questions and using out-of-wallet questions, and passwords are no longer enough—most of the items used to authenticate someone are readily available through the dark web.

The reality is that in 2018, 29% of Americans were victims of some form of identity fraud.

Approximately 30% of fraud victims experienced some form of account takeover.

The proliferation of synthetic identities and the anonymity afforded to online crimes heighten the risk of fraud losses. Customer contact centers need to adapt their objectives to meet the new realities. Contact centers are a treasure trove of information for criminals to gather what they need to take over an account.

WE ARE BEYOND THE CANARY IN THE COAL MINE

Customer service representatives are not trained fraud experts. They are experts in navigating multiple systems to quickly find and deliver information to the person making contact. Criminals are experts at navigating the helpful nature of contact centers to gain information and socially engineer enough data to take over an account or identity. The focus on conversational interactions—the outdated adage "the customer is always right"—and how agents are given incentives to quickly move through calls open the risk that too much information is shared.

The fact that financial services contact centers are PCI-compliant illustrates that being compliant with security protocols and data protection is not enough to thwart criminal behavior. Locking down internet availability, role-based system access, and masking data on the screens does not prevent social engineering. What has generally motivated financial institutions to invest in security technology is the identification of emerging threats such as malicious hacking and malware attacks.

- 54%: Addressing new risks
- 47%: Regulatory changes
- 46%: Improving customer and agent experience
- 45%: A security incident

It is now critical that operational and security teams realize that a security incident is taking place and is an active risk through social engineering in the contact centers.

HOW SYNTHETIC IDENTITIES WORK

Criminals purchase or otherwise source consumers' personally identifiable information.

This can include data from multiple individuals, including children (their SSNs are especially valuable).

A variety of data points are stitched together into a single identity and may be accompanied by fraudulent documentation.
This approach subverts traditional identity verification models by using credit reporting against FIs and issuers.

Recent U.S. legislation will eventually make synthetics ineffective, but they are still a major threat.

SOCIAL ENGINEERING IS HUMAN AND TECHNOLOGY ORCHESTRATED TOGETHER

Criminals have patterns when they take over accounts, generally making changes to personally identifiable information (PII) with the goal of being able to take funds or make transactions.

To make changes to the account information required criminals to resort to social engineering, in many instances through the contact center. Javelin Strategy defines social engineering as the combination of manipulation, influencing and deception, which results in obtaining information to take over an account. Because it is a three-pronged attack, multiple technologies and techniques need to be deployed to protect the contact center. The two channels most at risk are contact centers and digital banking chats (through mobile and online banking applications).

Manipulation—technical interference to mask the caller (phone number spoofing, computer emulation, voice morphing, SIM swapping).

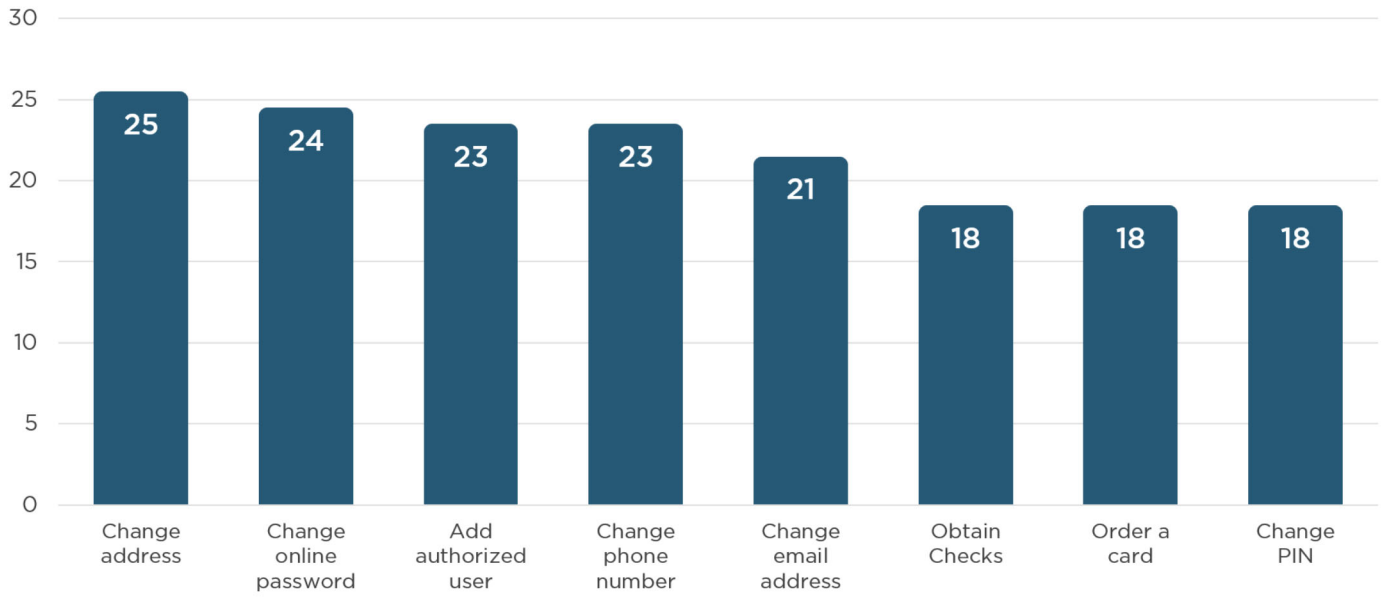
Influencing—extracting information from the representative through conversation (evoking empathy, explaining authorized user access, building a sense of obligation that assistance is needed, authority/tone of voice).

Deception—getting the true customer to do something based on being manipulated by phishing or scams or by someone they know and trust.

For details on how criminals can infiltrate digital channels, refer to the Javelin report ***The New Criminal Toolbox***.

Account Takeover Requires Criminals to Perform Multiple Activities

Figure 2. First Actions Taken by Criminals to Takeover an Account



Source: Javelin Strategy & Research, 2019

The human element comes in the form of deploying people to engage in social networks, call centers, and other contact channels to obtain information to elicit a payment or take over an account. Consumers are now used to robo-calls and are weary of voice-based scams; however, they do not have the same hesitancy online because a perceived relationship of trust has been established. The initial thought is that social engineering is the problem of the consumer (who should know better), but this is also a problem in contact centers. Not all contact is on the phone, and many are based on chat history. To take over an account and build trust, criminals can easily initiate simple inquiries and not immediately perpetrate fraud. The fraud can happen months later—when, needing to verify information, the criminal has all of the previous engagement history and can bypass standard authentication. Because chat is not currently the preferred method of engagement by consumers, they are unaware of the chat history and do not know someone is impersonating them to take over the account. Criminals have patience and will move toward the point of least resistance.

ADVANCEMENTS IN TECHNOLOGY IMPROVE SECURITY

The financial balance of spending money to add layers of protection compared with the increased rate of fraud due to criminals moving to the channel of least resistance should not be ignored. Contact center outsource providers, including payment processors and business process outsourcing (BPO), can provide some security but are generally limited to protecting the endpoint. It is up to the client—whether a financial institution or a merchant—to provide the consumer authentication and detection capabilities.

Throughout the lifecycle of contact, consumer expectations are changing to push financial institutions into "frictionless" experiences. However, friction is sometimes warranted to confirm the identity of the individual and reduce fraud losses. This delicate balance of visible and invisible security will bring contact centers a level of security previously not deployed. Due to the sweeping nature of the recommended changes, technology deployment will be staged to meet the evolving threat.

The goals of the contact center should remain consistent with the organizational mission and vision. However, consumers and agents have expectations that need to be met to make for an engaging interaction.

- Leverage predictive analytics and biometrics to identify criminals and recognize consumers.
- Connect systems to pass information seamlessly, reducing human authentication errors.
- Apply artificial intelligence across multiple channels to minimize threats.
- Provide confidence of protection and increase levels of trust from consumers.

How the technology is deployed will vary across organizations because of the number of platforms and providers engaged to service consumers. Ideally, each platform and provider would have the same technology; however, practical technology deployment across vendors will take time to scale and might not be cost-effective. Companies with operational systems deployed in cloud-based infrastructures will have a jump-start on deploying technology, as many of the solutions require robust data storage and analytic capabilities.

THE NEXT GENERATION OF CONTACT CENTERS

The challenges in managing contact centers and the consumer experience, balanced with mitigating fraud, is complicated by the fragmentation of service providers. Financial-services organizations may provide some call center services; however, third parties such as payment service providers, processors, and business process outsourcing firms provide many services for U.S.-based consumers. The shared-services model can provide significant cost savings and enable 24-hour servicing, but the ability to launch technology solutions across all channels at the same time is inhibited and not realistic. Making a priority of payment channels, followed by access channels, will enable financial institutions to make steady progress in reducing account takeover.

A missing component to the operational structure of contact centers is a dedicated fraud team that provides real-time assistance in the contact center to take high-risk calls, work cases created through new technology tools to identify fraud, and monitor calls for trends. In many instances, cases of suspected fraud are referred to the fraud team, either through a warm phone transfer or a follow-up after the fact. Having the option to use call routing from the interactive-voice-response (IVR) system on high-risk calls will assist in protecting the account and preventing fraud.

A general best practice for developing fraud management organizations is to create fusion centers, where people from different business lines come together to identify and reduce fraud. Because contact centers are managed primarily by third parties, it is important to bring representation to the fusion center or fraud organization but also retain fraud expertise on social engineering imbedded in the contact center.

To address the risks facing contact centers, organizations will need to realign the structure of the internal contact center and any outsourced partners that are used for servicing. Another component of the restructuring will need to be a holistic contact center strategy that centrally manages operations across payment channels. The increasing rates of account takeover and new-account fraud require a comprehensive approach that can unite card channels, loans, and demand deposit account access through similar processes and procedures. It may not be technically or organizationally feasible to develop a "super-agent," someone who can address all channels, or even access all systems, but the technology, metrics, and fraud mitigation devices should share intelligence regardless of channel.

The operational infrastructure to reduce the rate of account takeover creates new roles or realigns existing staff to create new groups. In addition to line-of-business oversight, the following three groups need to cross payment channels to address the full risk exposure of the financial institution.

Inbound fraud detection. Agents who can leverage cross-platform consumer access to monitor all accounts and reduce cross channel fraud.

High-risk call unit. Tenured agents who understand high-risk indicators and analytic outputs, requiring additional authentication before making account changes.

Dispute resolution. Agents who can handle not only Reg E and Reg Z disputes but also are required to

address the growing number of scams that involve different faster-payment methods (Zelle, Apple Pay, Google Pay, etc.)

Organizations need to have structures in place to manage internal and external activities to minimize fraud. Financial institutions and merchants are at risk for misalignment due to the multiple product lines and technology platforms required to operate an omni-channel consumer relationship.

INBOUND FRAUD DETECTION

When you hear the words "fraud detection," the image of groups of outbound call agents using a fraud detection system immediately comes into place. But fraud detection has changed with multiple channel interactions that reduce human interactions but make each one more valuable. When someone—either the criminal or the true consumer—wants to connect via chat, device or call, having the capabilities to quickly identify fraud coming into the contact center becomes a greater priority than the unit that places outbound contact.

Contact Center Toolbox

Multi-factor authentication call capabilities. Enabling voice over internet protocol (VoIP) calls when the consumer is authenticated in the application adds a greater level of security, especially when biometrics are used to access the app.

Screen pop and share. Not providing information from the initial engagement places the agent at risk of disclosing information to a criminal. Disconnecting the call and dropping the information may be the easiest and cheapest way to deploy contact center services; however, it is unsafe and causes consumer dissatisfaction when the true customer needs to repeat the same information. Computer Telephony Integration (CTI) is widely available but not often used.

Mobile push authentication. To confirm the identity of the consumer, initiate a mobile push notification to be sent to the primary registered device. Once the consumer validates the engagement, the contact via chat, call, or digital device (including voice) can continue.

HIGH-RISK CALL UNIT

Technology alone cannot minimize every threat, and not every high-risk interaction is fraud. To decipher the nuances of a valid authentication and a synthetic authentication, trained agents are needed. The high-risk call unit has a unique focus within the operational organization to minimize account takeover that occurs via social engineering and technology.

Contact Center Toolbox

Phone printing technologies. Real-time risk alerts and analysis to identify the validity of the communication initiated. Detect spoofing, synthetic voices, and behavior anomalies to provide instant feedback to agents about the risk of the call.

Natural language understanding (NLU). Leverage analytics to identify criminal behavior patterns across consumer identities and reduce account takeover risks. NLU can be used in IVR, chat, and contact centers, when all calls are recorded in a cloud environment.

Continuous authentication. Knowing the criminal patterns and behaviors is a key component in identifying fraud across multiple devices. Behavioral profiling of known bad behavior can minimize friction for true customers and divert engagements to a specialized unit when behavior is suspect.

DISPUTE RESOLUTION

Dispute resolution is more than having the ability to chargeback a transaction or represent information as a rebuttal. Consumers are consistently disputing transactions that may or may not have resolutions. The greatest threat is the digitalization of scams. Once originally thought of as fraud schemes where someone deposits a check, these crimes now involve managing contact centers to perpetrate scams against American consumers. The digital interactions can manifest as robo-calls, but they're more likely to be social-media connections that build a perceived layer of trust, leading to a digital payment. Transactions where someone is purchasing goods or services online using a real-time payment are irrevocable and lead to serious consumer discontent when they cannot get their funds back. Add in that social interactions are the foundation for account takeover, and victims of scams are at risk of account takeover.

Contact Center Toolbox

Next-best-action analytics. IVR, digital (mobile, online, and kiosk), and agent systems should enable identification of what is needed to resolve the dispute and protect the consumer. The key is not necessarily to reduce the average handle time (AHT) of an inquiry, (although it might) but to help the agent or consumer navigate a complex web of rights, responsibilities, and actions to minimize loss.

Case management systems. Extend beyond the card channel and migrate all payment disputes into one system to identify trends across consumers and channels, building comprehensive suspicious-activity reports that are actionable for law enforcement to engage and identify the threats. Leveraging API integrations to cross multiple platforms, investigations should move out of the payment channel and into one organization.

Interactive training technology. Guided learning during the conversation can help identify the root cause of the issue. Often, the consumer says there was fraud, but it could be a misunderstanding of policies or technology. Being able to demonstrate via mobile engagement during the contact session will provide one-on-one guidance on how to handle the situation.

PREPARING FOR TOMORROW'S CONTACT CENTER

From the site visits completed for this report, it is apparent that many companies have placed contact center security on the backburner because counterfeit card fraud is the priority. As fraud changes, financial institutions, merchants, and their service providers will need to invest significantly in the technology that protects their most vulnerable endpoints—humans.

Adding technology cited in this report will not be enough. The mindset of the organization needs to change from being transactional to focusing on relationships and engagements. The customer service models have changed—frictionless, omni-channel, and always available. The emphasis is on the customer always being right, solving a problem, or cross-selling different services. The engagement models of service have changed, yet security in contact centers is, for the most part, stuck in the 1990s. And as the complexity of servicing increases, expectations of agents to become generalists of all topics means that social engineering becomes easier and more prevalent.

Abdicating responsibility to the contact center vendor to keep the business secure and brand reputation intact opens vulnerabilities that cannot be managed without the client technology. More emphasis is placed on retaining business than on securing the business. When a business is vulnerable to fraud attacks, consumers lose trust. There is now a greater risk than the actual dollars lost when fraud occurs: the risk of consumers taking their business elsewhere.

METHODOLOGY

Javelin conducted tours of contact center facilities, speaking with executives within internal operations, and with business process outsource companies. Calls of conversations were evaluated to determine the ease of using authentication technology and to understand how key performance metrics were evaluated.

Fraud trend analysis in this report is based on a random-sample panel survey of 5,000 U.S. adults, fielded in November 2018.

- For questions answered by all 5,000 respondents, the maximum margin of sampling error is +/-1.41 percentage points at the 95% confidence level.

Organization spend and priority data in this report is based on information collected in a random-sample panel of 800 information technology security decision-makers, 200 of whom work in financial services.

- For questions answered by all 800 survey respondents, the maximum margin of sampling error is ±3.46 percentage points at the 95% confidence level.
- For questions answered by all 200 financial services respondents, the maximum margin of sampling error is ±6.93 percentage points at the 95% confidence level.
- The maximum margin of sampling error is higher for questions answered by segments of respondents.

The consumer payments data in this report was primarily collected from the following:

- A random-sample survey of 3,000 respondents conducted online in March 2019. The overall margin of error is +/-2% at the 95% confidence level for questions answered by all respondents.
- A random-sample survey of 3,000 respondents conducted online in October-November 2017. The overall margin of error is +/-1.74% at the 95% confidence level for questions answered by all respondents.
- A random-sample survey of 10,768 consumers in an online survey conducted in July 2017. The margin of sampling error is ± 0.94% at the 95% confidence level.