# TOP TRENDS IN IVR CONTACT CENTER FRAUD PROTECTION

Contact Solutions
A VERINT Company

Fraudsters are extremely clever and persistent. They're masters of deception who want to minimize their risk of getting caught – or even being detected. To succeed at authenticating and protecting your customers, you've got to stay one step ahead of the fraudsters. And in this game, prevention is a whole lot better than remediation.

So what's the next step ahead? Fraudsters tend to target customer channels what are overlooked, underdefended, or both to carry out their deceptive acts. That makes the contact center a prime target, where fraudsters have become increasingly sophisticated in how they attack the traditional voice channel with a new kind of one-two punch.

1 Deceiving **contact center representatives** is one tried and true method, but they are not the only targets of criminals in today's complex customer service environment.

2 The **interactive voice response (IVR)** system used by most contact centers has become a popular way to test out or validate account and personal information that fraudsters have collected through other means, and **find ways to sabotage and steal from your customers.**

For example, they can use robo-calling to try out thousands of different PIN numbers or other credentials in hopes of winning the jackpot. Unless multi-layer security measures are in place to detect, monitor and report these suspicious calls, fraudsters may have free rein to attack the IVR repeatedly, over an extended period.

Fraud is a growing problem across many channels, but contact centers – and their IVR systems – are trending to be targets of choice due to weaknesses ranging from complacency to legacy technologies. The IVR is a legacy, forgotten technology that deserves attention as it gains popularity as a channel for fraud. It should be protected as far upstream in the cycle as possible – before fraudsters can insinuate themselves into customer accounts and steal money, benefits or personal information.

These articles summarize how to identify growing fraudulent trends in the IVR, and how to address this escalating problem now.

# HOW MODERN FRAUDSTERS WORK THE CONTACT CENTER

by Tim McCurry,
Contact Solutions,
a Verint Company

Large data breaches, of which there have been many lately, are usually just the beginning of rampant credit and debit card fraud. During these breaches, the goal is to steal as much personal customer information as possible. While customers may feel relieved when a data breach exposes only personal contact information such as name, address, e-mail and telephone number but no financial information, it's critical to understand how criminals use this personal information to gather the missing pieces of information.

In cases when criminals do hit the motherlode of card or account information including social security number, account numbers and card numbers, they still lack personal identification numbers (PINs) since those are not stored on the card. While they can perpetrate fraud without the PIN, a PIN will give them access to cash at the ATM. Now, it's time for them to get busy and start collecting the information they need to complete the fraud.

It's critical to note at this point that no company is immune. Larger companies – witness the hacks of Home Depot and Anthem – may attract more attacks simply because of the volume and sensitivity of the customer data they hold, but smaller companies aren't off the hook, either. Most companies, regardless of size, maintain information that is of at least some value to fraudsters, and these companies are often considered "easy marks" by hackers because of their lack of sophisticated security barriers.

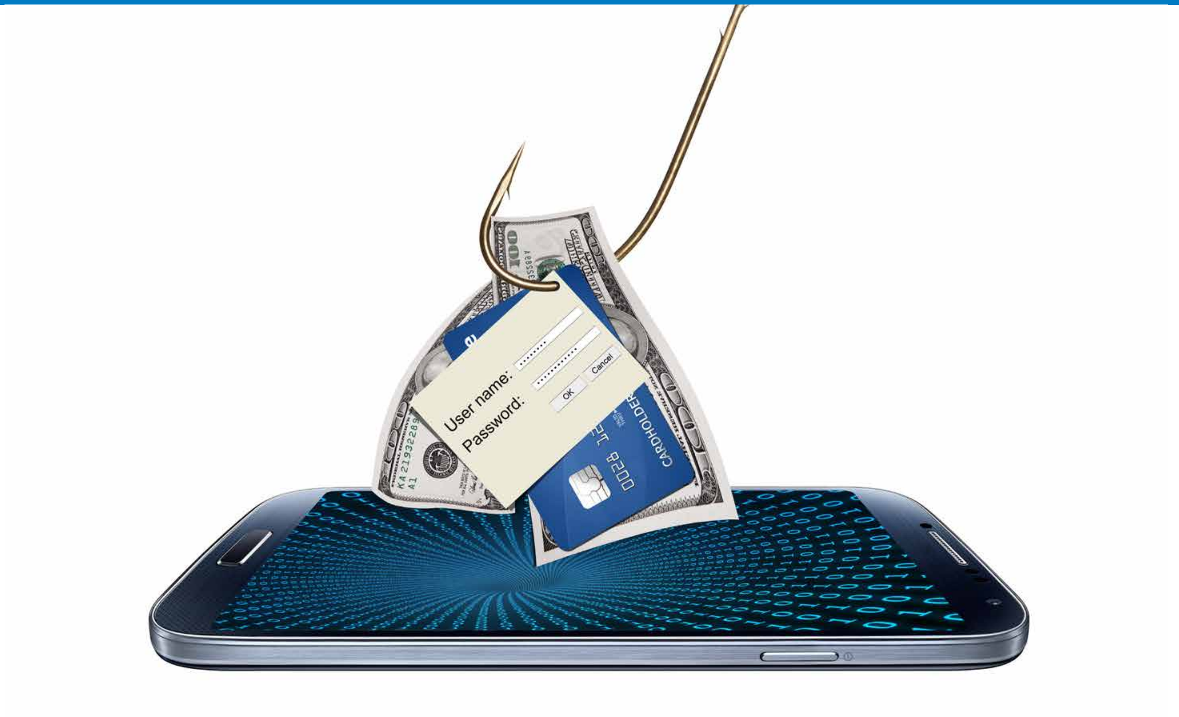
.

## The Fraudulent Company Call Angle

To aggregate the information they need to completely compromise an account, the criminals will go to work posing as company representatives. They will call victims and claim to be employees at the customer's financial institution. While most people have been told never to hand out personal information to "company representatives" who call claiming to be from a bank or any other business claiming an account or personal relationship, fraudsters have many advantages to skirt that issue and convince unsuspecting consumers to give up their personal, confidential information. They sound professional, and they already have a lot of a customer's personal information, making them seem legitimately calling on the consumer's behalf.

*Good morning. This is John Smith with ABC Bank. We were going through your account information and saw some discrepancies. I'm calling to ensure that your information is up to date. I have your name, your address and your e-mail, and your account number as 12345678. Just to confirm all this is correct, I just need you to enter your PIN.*

The customer, confident the call is legitimate (after all, if it wasn't, the caller wouldn't have all that personal information, right?) enters his or her PIN, and the fraudsters now have everything they require. They can make a duplicate card from nearly any card with a mag strip – hotel key cards are popular – and either sell the cards or go shopping. One common practice is to use self-checkout kiosks at retail stores such as Walmart to buy gift cards and then resell those cards.



## Fraud in the Contact Center's IVR

Now that the criminals have gathered PIN numbers, they will look for the most convenient automated process – which tends to be the contact center's IVR — to try and use the information they've collected to their advantage. They can use the IVR to check balances and pending deposits to determine when the most lucrative time to clear the account will be, and then perpetrate fraud by purchasing something via the internet or over the phone (known in the industry as a "card not present" transaction), creating a counterfeit card or engaging in an account address change and having a new card sent to that address.

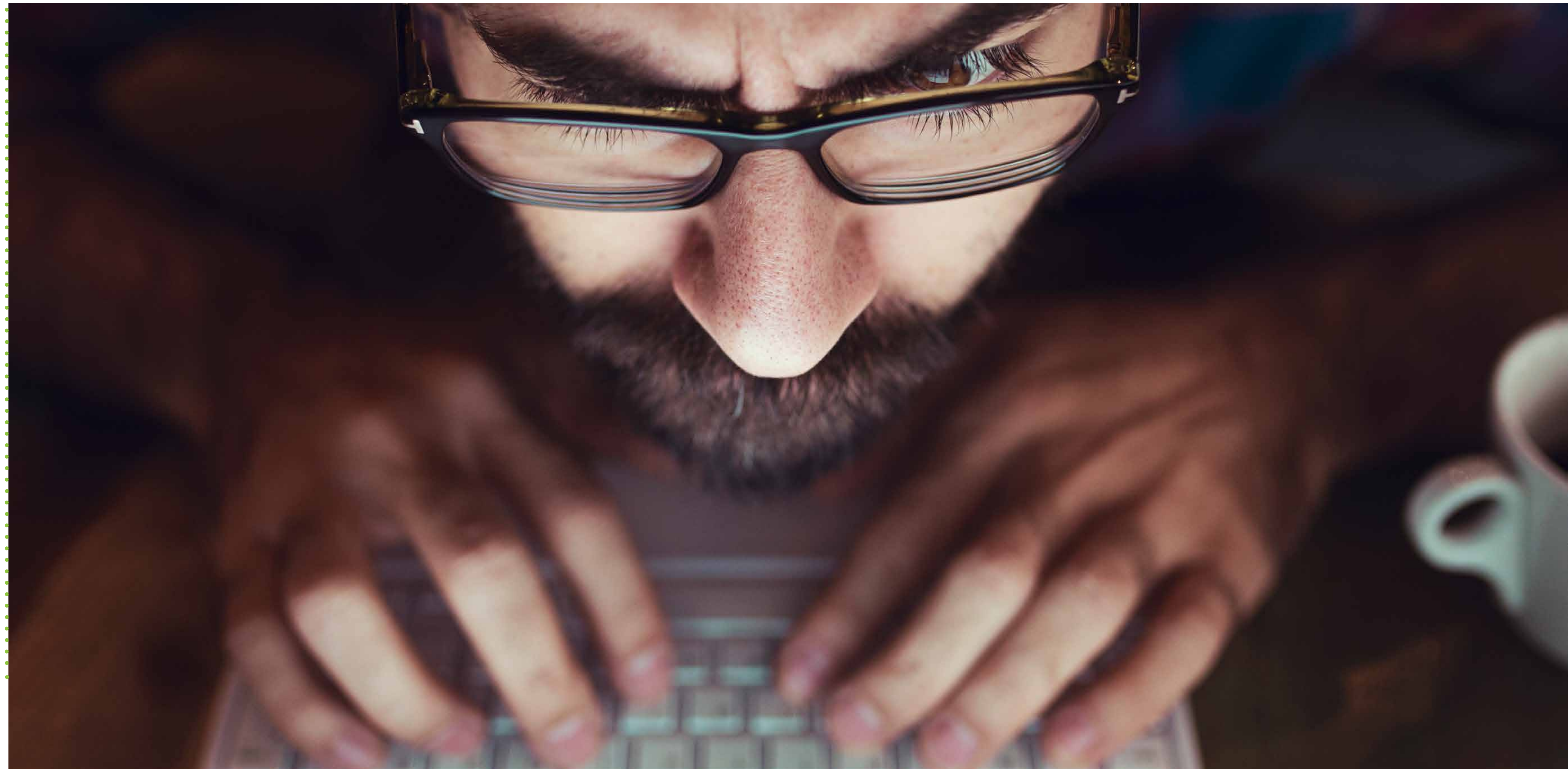
If the fraudsters have some but not all personal information, the IVR becomes a method for them to validate the information they have, and probe for additional information. If they have an account number, a social security number and a date of birth, but no PIN, they can engage in a brute force attempts by repeatedly calling into the IVR and guessing various PINs (too many people still use obvious numbers such as birth dates for PINs). Alternatively, they can reach a live agent and pose as a customer in an attempt to squeeze information out of the agent, or ask to reset a PIN. Fraudsters will often call back until they reach a lesser-trained, more sympathetic agent who will fall for a sob story ("I'm stranded in an airport and my PIN isn't working!") or be persuaded that the caller is legitimate (after all, he knows a lot of personal information about the customer, so it must be the customer himself, right?). If agents seem confident that the call is truly the customer – and fraudsters are very good at making it seem so – the agent may provide the missing information or approve a new card to be sent to a new mailing address.

Working through live agents presents a risk, however. Agents may notice a pattern of repeated calls, and better trained agents may report instances of probing as potential fraud. For this reason, the IVR remains a favorite tool of crooks precisely because it's impersonal, automated and, in many cases, not monitored for patterns of fraudulent behavior. It provides critical information — balance and deposit data — quickly and easily, supplying crooks with all the information they need to drain an account at the most lucrative time. For this reason, the IVR is a critical place to halt fraudsters engaging in phishing, probing and validation activities in their tracks. Many organizations don't realize how ill prepared they are to handle this ever-changing, complex fraud channel and may not even realize the volume and scope of fraudulent activity taking place right now on their watch.

## A Highly Organized Criminal Enterprise

While we may preserve a mental image of a cybercriminal being a poorly socialized individual operating from a dim basement for personal gain, the reality is that global financial cybercrime is big business. Stolen card data from large scale (and even not-so-large scale) data breaches is highly profitable. Criminals collect the card information, separate it by bank based on the bank identification numbers, or BINs, and sell this information in bulk to organized criminals.

According to the Identity Theft Resource Center, some groups — Eastern European criminal enterprises, for example — will offer for sale on the black market a "bucket" of Citibank or Bank of America cards, with prices varying depending on the amount of information available. Costs will run between $8 per record for card information — which requires more footwork to use — to $30 to $40 for a complete dossier of personal information including social security numbers, names and birthdates. With the latter information, fraudsters can simply open a new account in a victim's name.



## Multi-channel Fraud

As businesses have gone multi-channel with their support, so too have fraudsters. Today, they have a variety of channels open to them to collect information, put it all together and take over an account. Social media can be used to validate information, and criminals are bold and skilled enough to contact their victims directly to phish for missing information. Once they have collected everything they need, they simply head to the call center or the IVR to complete the account takeover.

As fraud has become more complex and multichannel, stopping it also needs to be a process with multiple layers. Today, companies need to be proactively tracking and monitoring activity and taking a variety of active steps to stop the criminals. There is no “one size fits all” answer, or magic shield – like Harry Potter’s invisibility cloak – that will do the trick. To improve business processes, protect customers and guard against multiple types of breaches, organizations today need to be thinking about the variety of ways they can stop different types of fraud.

In the call center, this means building a multi-layered solution that offers a combination of safety measures that works on both the customers’ and company’s behalf. An effective and more cost-effective option is to include automated ANI (automatic number identification) verification, behavioral analytics and the ability to identify red flags in real-time, and automated knowledge-based authentication options. These safeguards, often put in place for calls requiring live agent assistance, must also be applied to the IVR, where no one is actively watching and criminals are counting on this fact. Adding security to live call center channels but ignoring the IVR is a bit like guarding the front door but leaving the windows wide open. No company wants to be the one robbed by fraudsters who used the company’s own customer support technology against it.

Stopping financial cybercrime is one the largest challenges to global business today. Criminals are highly adaptive: shut down access to one piece of information, and they will simply change their tactics and find another way to get in. Industry experts have asserted that an organization must continually shift their own tactics when it comes to fraud prevention. What this means is that fraud protection is a living, breathing process that must grow and adapt, and any solutions chosen to protect the organization must do the same

.

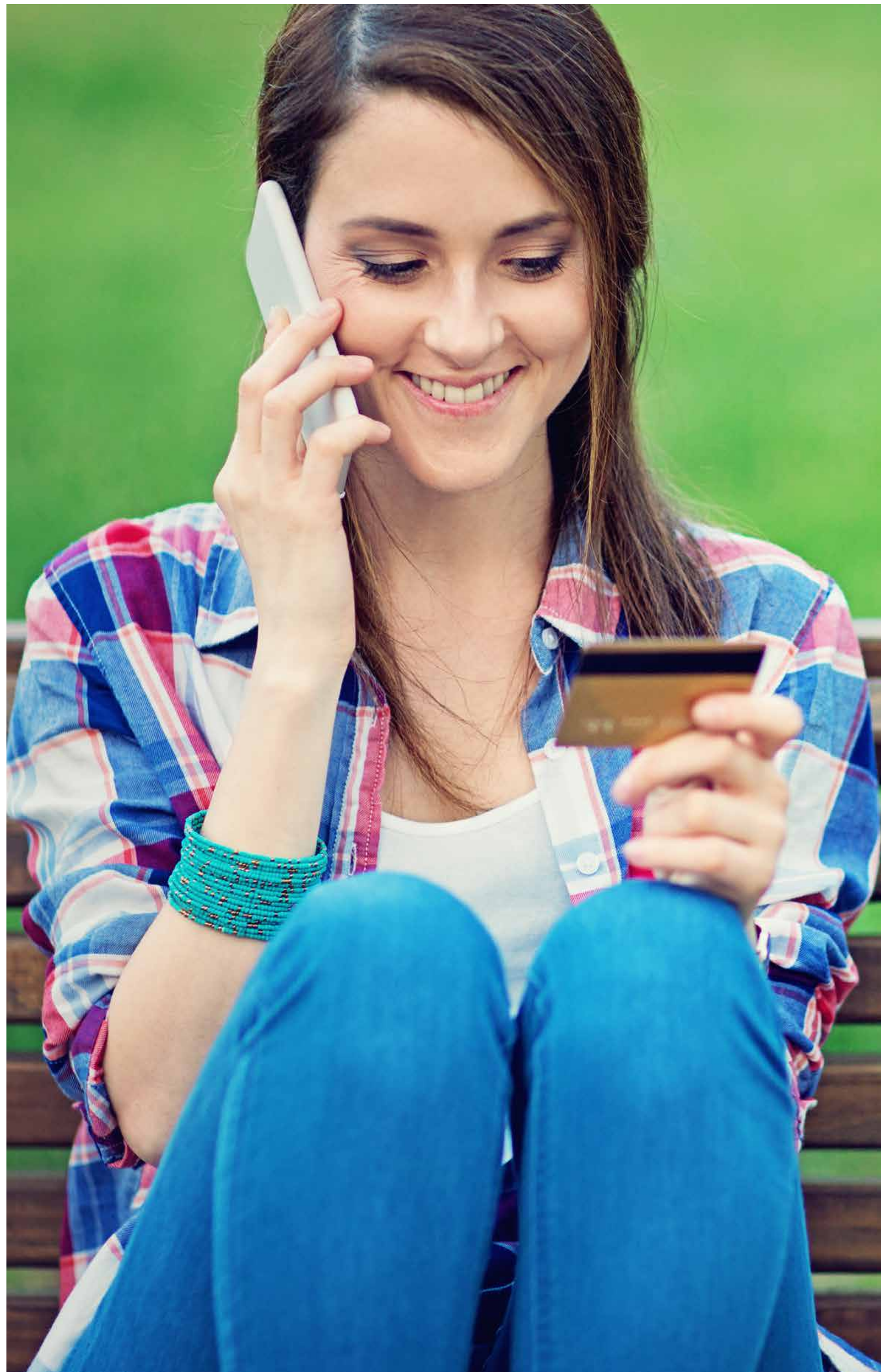
# CATCH CONTACT CENTER FRAUD UPSTREAM IN THE IVR BEFORE DAMAGE OCCURS

by Andrea Katsivelis,
Contact Solutions,
a Verint Company

Fraud occurs every day and impacts the enterprise and the consumer. In fact, it's so prevalent I can't remember a time — certainly not in this decade — when fraud wasn't a top-of-mind issue in our lives. But what happens when fraud impacts business on your watch, and you were certain you took every conceivable precaution to ensure it wouldn't and couldn't happen? There's a missing link in fraud prevention, and it just may surprise you.

## Consider a Day in the Life of Your Customer

- Your customer may call your customer care line to check a balance, make a payment, get support on a product or issue, or more.
- He or she has done all they can to previously establish passwords and PINs with you, and now they rely on you to ensure their personal information and their account is safe in your hands when they initiate their call.
- Your customer first reaches the IVR to authenticate and manage their needs on their own – in fact they prefer self-service to expedite the interaction unless there is a more complex reason to speak with an agent.
- The customer validates properly, completes their transaction, and goes about their day.



## Now…Imagine a Suspicious Call into Your Contact Center

- A man with a heavy foreign accent on a poor-quality VoIP call claims to be a 73-year-old retired teacher from Dubuque named Myrtle Henderson.
- As part of your authentication screening, “Myrtle” fails a step and is sent to an agent for further authentication. Poor dear, fake “Myrtle” explains, “I’m sorry, but I’ve forgotten the name of my first childhood pet. Silly me. Can you help?”

## Now consider how that call can go

There are two kinds of contact center agents: the sharp ones, who will smell a fish, and the naïve ones, who will assume that Mrs. Henderson simply has a bad cold and a failing memory when it comes to dear, departed Fluffy. Which kind of agents do you employ? Do you pay them enough to care?

While some agents are capable of picking up on suspicious calls, others may be too busy or too poorly trained to do so. Remedial training for agents can help cut down on fraud attempts through live voice calls, but it won’t do anything to keep criminals from probing automated channels.

## Handling Fraud Downstream Is Like Locking the Doors after the Burglar Has Already Taken the Flat Screen

While larger companies today focus their efforts on online user authentication and verification for critical transactions like electronic funds transfers, they pay little attention to authentication and verification in the contact center beyond the contact center agent. While passive voice biometrics during an agent interaction and other tools are extremely valuable deterrents, they should not be used alone.

If a fraudster makes it through one or two layers, the remaining layers and measures can help backstop the others and prevent an attack from succeeding. If the correct measures are taken to protect the customer **upstream**, then customer support organizations can avoid the damaging fallout that takes place downstream, after the fraud has occurred.

## Stop Fraud Upstream in the IVR Before a Loss Occurs

In the contact center, traditional fraud detection tools (if they’re present at all) are put into action downstream to deny transactions at the last moment to avoid a loss, or identify losses after they have occurred for future prevention. They include transaction processing solutions that flag suspicious purchases, cyber security issues to prevent digital interaction and data compromise, and network or data center security to block breaches.

By concentrating fraud prevention efforts upstream, before a criminal can complete an account takeover or other fraud, organizations can prevent the costly fallout and loss of customer goodwill that can result from breaches.

Since the IVR is where a lot of contact center fraud begins today, it makes sense for companies to put an IVR in place that can spot fraud attempts before they can cause damage, and stop them.

## Upstream protection in an IVR requires a solution that can do a number of things at once:

- Monitor caller behavior
- Provide heightened authentication
- Detect and stop probing activity in the IVR
- Reduce fraud losses and prevent account takeover
- Deliver convenient self-service that saves time and effort

Essentially, it involves a change in strategy, pivoting from reaction to prevention. Using adaptive fraud prevention technology, contact centers can detect and prevent fraud upstream in the IVR before loss occurs.

To be truly effective, the solution must:

- Require the collection of data at every interaction point in real time.
- Demand that the data analysis be immediate and ongoing – to quickly and effectively identify fraudulent activities that are actively occurring and take action as fast as possible.
- Provide a multi-layered approach that fits the needs of the organization, transaction types, and customer base served.
- Deliver immediate action – best determined by the client needs – with the ability to take different preventative steps appropriate to the circumstances.
- Ensure client insight and decisioning capabilities that align with other existing fraud management activities.
- Continue to learn and apply protection over time as changing behavioral, reputation, and knowledge data are collected and applied.

# PROTECTING GOVERNMENT AGENCIES FROM FRAUDSTER ATTACKS

by Tim McCurry,
Contact Solutions,
a Verint Company

People who take part in Government programs are prime targets for fraudsters waiting anxiously to grab-n-go their valuable information and funds. Crooks from around the world use a range of tactics to acquire personal information so they can take over a constituent's account to steal benefits or payments.

Clever fraudsters often target the interactive voice response (IVR), a gateway used by many government programs to provide automated self-service and a path to live agent support.

Here's how fraudsters try to beat the system:

- They obtain a constituent's personal information from health records, data posted on social media, or old fashioned mail theft.
- Pretending to be a government program representative, they may contact the constituent to "validate account information." The person is persuaded to reveal confidential information that can be used to unlock their accounts and steal funds.
- The fraudsters call the government program's contact center and attempt to take over the constituent's account based on this identity information. Many interactions take place via the IVR, while others involve speaking with an agent.

## Multiple tactics demand multi-layer protection

Fraudsters are not only diverse—ranging from individuals to international gangs—but also use many different tactics to steal constituents' information, benefits and funds. These people are smart, creative and incredibly persistent. They will eventually find a way to defeat **any single defense** against identity theft.

That's why Government agencies and programs need a multi-layer, adaptive approach to identify and stop fraudsters before they can take over constituent accounts via the IVR or by fooling a contact center agent. Such a solution should target three aspects of fraud:

- **Phone number reputation:** This layer of the solution automated in the IVR compiles a database of phone numbers used by callers to the IVR, including geographic locations, network providers, phone types and any fraud activity history. It assigns a reputation score that can be used to flag suspect numbers. The solution also targets call spoofing, voice distortion and other tactics used to trick the system.  For example, VoIP calls can indicate a suspect call. Only 1 percent of legitimate callers use VoIP, as opposed to nearly half of fraudulent callers. And while 10 percent of legitimate calls are international, about 40 percent of fraud calls come from another country.

- **Behavior patterns:** Based on huge volumes of behavioral data generated by the IVR, this layer uses data mining, algorithms, and other tools to identify, prevent, and/or control unusual caller behavior in real time. This approach helps detect and deter fraud activity before a transaction can occur.  On average, a fraud attack comprises five IVR calls – the majority for surveillance, data gathering and probing – before the account is breached. This suspicious behavior can be detected and dealt with using the technology described above and below.

- **Knowledge-based authentication (KBA):** The third layer is constituent authentication based on a dynamic set of automated questions derived from public sources. Instead of having a contact center agent read a questionnaire to the caller – a time-consuming and expensive process – KBA is integrated into the IVR workflow using automated questions with multiple-choice answers. If the caller passes the test, he or she advances to the next step.  KBA stops fraudsters before they reach a live representative, helping to avoid the use of verbal coaching or persuasion that can result in a successful attack.

## Thousands of Fraud Calls

**A typical medium-sized government contact center can receive three dozen fraudulent calls per day, adding up to a thousand each month.** Fraud not only hurts vulnerable constituents by depriving them of much-needed funds and benefits, it also impacts the program or agency's reputation and can quickly add up to millions in losses.

# TIPS FOR CONTACT CENTER FRAUD PREVENTION

by Andrea Katsivelis,
Contact Solutions,
a Verint Company

Fraud presents a major threat to both the consumer and your business. Some tips to keep in mind:

1. **Fraud is more dangerous than ever before.** There is at least one mega-breach per quarter, with greater than 10 million customer records compromised, and the FBI estimates that more than 1,000 retailers are currently under assault with the same malware used in the Target breach.

2. **Fraudsters make more than 1 million calls per month, and can cycle through phone numbers on an average of every two weeks.** Fraudsters are sophisticated and persistent, and they will continue to attack in every way possible.  While this number may change depending on an organization's individual customer data, many organizations don't even have a clear view of where they stand.

3. **Multi-layered prevention is the best way to manage fraudulent activities while enhancing customer satisfaction.** Even if a fraudster gets through one or two layers, it's unlikely they'll be able to continue through all of them. Combining behavioral, reputation, and knowledge fraud prevention techniques is a perfect example of how to implement this.

4. **Fraudsters can use a variety of methods to target your organization.** Use an adaptable approach to combat them – one that changes as quickly as the fraudsters' methods. There is no one-size-fits-all approach.

5. **The best way to prevent fraud in the contact center is to automate fraud prevention tools in the IVR.** Highly advanced tools incorporated into the call flow and authentication processes. can help you reduce costs, minimize the burden on your callers and your agents and stop fraudsters in their tracks.

**Learn more about automated authentication and fraud prevention in the IVR at http://info.contactsolutions.com/contact-center-fraud-prevention-ivr**

**About Contact Solutions, A Verint Company**
At Contact Solutions, we believe customer engagement should be effortless for the customer and sustainable for the enterprise. Our cloud-based, voice and digital customer engagement solutions reduce effort through highly personalized self-service and agent-assisted experiences, provided at the convenience of the customer. We use business intelligence to continually improve and optimize customer care so enterprises can achieve superior results at sustainable cost, while adapting quickly to rapidly changing customer demands.

**Verint. Powering Actionable Intelligence®**
Verint® Systems Inc. (NASDAQ: VRNT) is a global leader in Actionable Intelligence® solutions for customer engagement optimization, security intelligence, and fraud, risk and compliance. Today, more than 10,000 organizations in over 180 countries use Verint solutions to improve enterprise performance and make the world a safer place. Learn more at www.verint.com.

PUBLISHED 04/2017

www.contactsolutions.com • information@contactsolutions.com • 1.866.979.3339