2018
VOICE INTELLIGENCE
REPORT
A review of fraud, the future of voice, and the impact to customer service channels
With physical and online information security always growing stronger and harder to crack, fraudsters gravitate toward the weakest link in your security—your contact center and voice channels. For many years, our annual fraud reports have shown that fraudsters increasingly exploit the phone channel. Fraud rates continue to increase every year, and this year is no different.

Between 2016 (1 in 937 calls) and 2017 (1 in 638 calls), the overall voice channel fraud rate increased by 47%, continuing on the upward trend from last year 113% increase. From 2013 through 2017 we have seen the fraud rate climb over 350%, with no signs of slowing down. It is important to note, that some verticals (i.e. Retail) experience even higher fraud rates than shown here.

This report will explore and analyze these numbers, provide additional data about global voice channel fraud rates, offer some analysis about the “why” behind these numbers, and how to mitigate against the increased fraud rates.

Specifically, this report will discuss:

- Why the fraud rate continues to increase despite more security awareness than ever.
- How advances in AI and machine learning not only help businesses serve customers but are also exploited by fraudsters who leverage advances in technology to create more sophisticated, emerging fraud tactics.
- How many businesses feel disincentivized to add stricter call center security measures, as they feel that anti-fraud and authentication efforts using current technology backfire and negatively impact customer service.
- How specific industries struggle with unique fraud problems and fraudster strategies.
- Proactive measures to protect against fraud threats (both conventional and emerging).
PART ONE:
Why Does the Fraud Rate Continue to Increase?

A perfect storm of four key events has led to a steady, sharp increase in year-over-year phone channel fraud.

1. EVERYBODY’S DATA HAS BEEN LEAKED IN A BREACH

The Identity Theft Resource Center reports that the “number of significant breaches at U.S. businesses, government agencies, and other organizations topped 1,300 last year, versus fewer than 200 in 2005.” Anecdotally, stories of major data breaches now regularly make national news. Something as significant as 10 million records being released surprises no one. Data breaches are now mainstream. Fraudsters are increasingly using this data to ‘phish’, or trick into revealing online, genuine customers. Fraudsters then use that data for account takeover attacks.

The trend continues to increase, and data breaches aren’t going away.

Why? Cybercrime is a $1.5 trillion “industry”—more profitable than the drug trade. This profitability attracts incredibly sophisticated fraudsters who run their criminal organizations like finely-honed businesses. This sophistication means they are pragmatically assessing organizational weak points and exploiting them. Cybercriminals are not just trying one tactic, such as online hacking. They are exploiting the phone channel, often the weakest link, and using a multichannel strategy to commit data breaches.
2. FRAUDSTERS GO OMNICHANNEL

Despite specific increases in voice channel fraud, our numbers likely do not represent the total increase due to the difficulty of tracking cross-channel fraud. Fraudsters use all available channels to achieve their goals. As fraudsters grow more sophisticated, they often originate fraud in one channel and commit the actual fraudulent transaction in another channel.

For example, a fraudster may use social engineering to reset a password on a victim's account. Then, they can use that reset password to commit online fraud. An example like this shows the difficulty in identifying interactions that lead to fraud. Many cross-channel steps can appear like a legitimate transaction and make fraud harder to spot. For one particular voice channel, Pindrop’s research showed that over 60 percent of the confirmed fraud calls were information gathering by criminals to achieve fraud in the online channel.  

IVR FRAUD CASE STUDY

Precrime is not just for the movies anymore.

On one anonymous Fortune 500 customer environment, Pindrop conducted a forensic investigation of fraud in the IVR, the phone channel and the online channel. Pindrop Labs found that suspicious activity in the IVR is the leading indicator of cross channel fraud. On average, suspicious IVR activity resulted in a fraudulent transaction attempt 15 days later. For more than 85% of fraudulent transactions that originated in the IVR, we had a 24 hours lead time. This gap in the IVR activity and the actual fraud is evidence of a very common occurrence in the fraud landscape. One fraudster might purchase a list of compromised accounts on the dark web, and use the IVR to identify which accounts on his list are still active. With that information, the fraudster can prune his list and resell it. Lists that are demonstrated to have higher amounts of active accounts sell for more money on the dark web. This simple task allows this fraudster to profit from data breaches, but not take the risk of getting caught committing actual fraud.

In addition to financial losses, data losses are also a concern with cross-channel fraud. For example, a fraudster might socially engineer a customer service representative in a telecommunications call center to gather information, take over an account, or access a victim’s email. While no money gets stolen, the data breach is a huge incident for that telecommunications company. By the time the data breach is detected, it may be too late as criminals use the stolen information or account takeover to steal funds from another institution (such as a bank).

CONTACT: 866.245.4045 | info@pindrop.com

© Pindrop, 2018 | www.pindrop.com | 2018 Voice Intelligence Report

4 Contact Centers: The Fraud Enablement Channel, Aite Group, April 2016
As fraud becomes more cross-channel, it becomes more cross-industry. Even if fraudsters aren’t stealing money in a particular industry, that doesn’t mean data breaches are any less serious. A data breach is usually one step away from financial loss. Similar to why they exploit the weakest channel (voice), fraudsters exploit industries with weaker security and then use that data to breach industries with stronger security (such as banks).

**CROSS CHANNEL FRAUD EXPANSION**

- **Web & Mobile Security**
  Strong web controls can mitigate some fraudsters from taking over weak accounts and moving to the phone channel.

- **Omni Channel Voice Security**
  As channel boundaries blur, persistent customer authentication and anti-fraud protection will need to grow to counter expanding cross channel fraud.

- **Call Center Security**
  Anti-fraud and authentication in the call center can keep fraudsters from resetting passwords and using credentials for web and mobile apps.

- **Anti-Fraud**
  - Web & Mobile
  - Voice Channel
  - Call Center

**Cross Channel Security**
Fraudsters who trigger security mechanisms in one channel will hop to a channel with less security controls.

**3. BREAKING UP (WITH KBA QUESTIONS) IS HARD TO DO**

Despite increased data breaches and sophisticated cross-channel attacks, businesses have mostly remained stagnant when approaching phone channel security. Identity verification still largely relies on easily accessible KBA questions such as asking for your mother’s maiden name—even though this is now readily available information on the dark web. “Something you know” questions are no longer secure when more than one person has the same information.

Yet, many organizations use KBA questions out of ease and habit. Even organizations that have implemented some form of advanced authentication with positive voice bio or one time passwords, fraudsters are at the ready to social engineering call center agent to convince them why they are unable to authenticate, such as a lost phone, a sore throat or background noise. These tactics are all geared toward getting back to the KBA questions they can answer.

**4. BETTER MOUSETRAPS CREATE SMARTER MICE**

As businesses embrace new technologies, fraudsters do the same. Many experts view cybersecurity as an arms race that we’re losing. Fraudster tactics work, and fraudsters continue to evolve and adopt new technology to enhance and streamline criminal activity.

This technology arms race always seems to leave a slight edge to the fraudsters. Some of their evolving tactics include beating advanced single-factor authentication security measures and getting past traditional single-factor voice biometrics obstacles.
To get past voice biometrics security, fraudsters are using the following tactics:

**Imitation:** An attacker may try to impersonate the legitimate speaker or disguise themselves to escape a positive identification.

**Replay Attack:** A fraudster simply records the target victim’s voice such as getting on the phone with them for a few moments or even looking up a video online where they may be speaking. With a replay attack, there is no need for social engineering or imitation, and the quality of the voice can be quite high depending on how the fraudster acquired the voice sample.

**Voice Modification Software:** This is software that converts a fraudster’s voice to match their victim’s voice through the use of features such as electronic pitch control.

**Voice Synthesis Software:** In an era of “fake news,” voice synthesis is raising ethical concerns over how easy it becomes to imitate a human voice. Lyrebird just needs a few minutes of audio to recreate a voice avatar. Obviously, fraudsters will take advantage of software such as this to create near-accurate versions of a victim’s voice.

Even for companies trying to avoid the voice channel, the alternatives aren’t any more secure. Fraudsters have become good at exploiting the security weaknesses of Interactive Voice Response, or IVR technology and chatbot programs. Unmonitored IVRs are a rich knowledge base for fraudsters who use robocall dialing to verify information, verify PINs, and collect balances. Again, data fraudsters can use this information to steal money elsewhere.

---

5 https://lyrebird.ai/
PART TWO:
AI Disrupting the Voice Channel

In a April 26, 2018 Forbes article, author Gil Press summarizes a Forrester report when he says: “Forrester outlines a number of ways in which cyber criminals will profit from AI in the immediate future, including automating attacks and significantly improving the targeting of victims; better impersonating individuals for more effective social engineering; creating and targeting fake news; better code and better use of attack resources for distributed denial of service (DDoS) attacks; and developing more virulent malware and viruses.”

AI presents exciting but uncharted territory. Like any disruptive technology, benefits exist for businesses alongside opportunities for criminals to use this technology against us.

SYNTHETIC VOICE ARRIVES

In the category of AI, synthetic voice is probably one of the most exciting, and potentially the scariest. Right now, Google Duplex merely aims to help automate simple tasks like booking a restaurant reservation using a synthetic voice based on a real person. Inevitably, this technology will evolve into uses more complex than snagging a table for brunch—and with that evolution comes privacy and security concerns.

Obviously, fraudsters will take advantage of this advanced technology and exploit synthetic voice. Instead of calling for a brunch reservation, fraudsters may use your hacked Google Assistant to transfer funds from your bank account to a fraudster’s account.

Businesses already use machine learning for device, behavior, and voice matching. But fraudsters remain slightly ahead—using machine learning to create synthetic speech, spoof ANIs or CLI, and conduct robocalls to mass attack and spider through an organization’s IVR in order to verify stolen account information.

CHATBOTS BECOME THE NORM

With improvements to AI come improved chatbots that can take over many aspects of a CSR’s conversation. Because chatbots automate many routine calls and conversations, more and more businesses obviously want to explore its use. In fact, Gartner predicts that customers will manage 85 percent of business relationships without humans by 2020.

Because so many chatbots are unmonitored, fraudsters abuse them with fervor—conducting reconnaissance like how they approach unmonitored IVRs. As businesses implement more chatbots and AI capabilities to improve customer service, security must be built from the ground up. Otherwise, businesses give fraudsters many opportunities to commit fraud.

“Sins of the past” worsen this problem. Because businesses have used KBAs for so long, fraudsters now have plenty of access to these authentication answers from massive data breaches. Fraudsters then use these answers to hack new channels such as chatbots.

---

2 Bohn, D. (2018 June 27) Google Duplex really works and testing begins this summer, www.verge.com
THERE IS A LEAK IN THE IVR

As more and more companies start to leverage chatbots and AI to offer self service to their customers, security must be top of mind at every access point. The newest trend Pindrop Labs has found, something called brute force attacks, involves using bots to programmatically use an unmonitored IVR to test and check combinations of account numbers, passwords and birthday and deliver the final results back to the programmer.

Fraudsters can also use artificial intelligence to test account numbers at random, instead of sequentially which could trigger an alert. Because these systems are often unmonitored they are an effective resource for fraudsters using advanced technology to perform account reconnaissance.

Detecting fraud in an automated system can be difficult to detect. Many times customers will have more than one account or have multiple phone numbers tied to one account. Without the ability to tie phone numbers to account in automated systems, a large potential blind spot in the organization develops. The IVR was supposed to be a device to increase self-service to help check account balance checking or reset passwords, now allows access for fraudsters to create their own ‘fraud network’. Multiple phone numbers logging into a single account, fraudsters adding additional numbers associated to an account they have taken over, could be the same number that is attacking more account. This cumulates in a single fraudster taking over multiple account in one institution.
PART THREE:
Security’s Impact on Customer Service

A major reason that fraud rates increase is that most organizations struggle to find the right balance of security and customer service. When stronger traditional security measures are put into place, these measures typically impact customer experience—often to an organization’s detriment.

Some industries are disincentivized to deal with the negative costs related to anti-fraud and authentication solutions. What happens when the cost of fraud is less than the cost of customer churn and lost revenue from the negative side effects of heavy-laden authentication procedures?

For example, false declines or not processing a transaction due to suspicion of fraud, cost the retail industry an estimated $8.6 billion in 2016 in the US alone. The fraud losses prevented by these measures? $6.5 billion. Doing the right thing is costing the US retail industry $2.1 billion.¹⁰

Yet, this doesn’t mean businesses can simply slack on data privacy and security. Existing laws, regulations, and policies grow stronger every year as data breaches become more of a national security issue (rather than just an issue for individual companies). The EU General Data Protection Regulation (GDPR), for example, not only affects the data of EU residents but its ripple effects have led many companies to apply GDPR’s privacy standards to all users (rather than segment out privacy standards for some users and not others). Recently, from public pressure and increased awareness after the Equifax data breach and the Facebook–Cambridge Analytica data scandal, we have seen passage of the California Consumer Privacy Act. Further, the White House has recently shown a new openness to data privacy standards where before there was little interest.¹¹

These national and international trends in privacy laws and regulations, along with the fallout from data breaches and scandals, has increased the expectation that companies keep data safe, be transparent about how they use customer data, and increase the amount of public trust and understanding about data use, privacy, and security.

This puts businesses in a difficult but inevitable spot. Even if they slack on strengthening anti-fraud and authentication measures with the rationale of saving money, businesses risk a more painfully expensive data breach. A data breach not only impacts companies directly (stolen money, notification costs, forensic investigations) but also indirectly (loss of shareholder value, loss of revenue, loss of brand reputation). Yet, consumers want speedy, frictionless customer service processes—and competition often drives these processes as a priority over security. Customers also frequently choose convenience over security (weaker and/or repeated password/phrases) reducing the effectiveness of business’ security methods.

“We have always been bullish on streamlined authentication for our customers. Pindrop allowed us to achieve the trinity of higher customer satisfaction, reduced agent time, and further reduced fraud.”

- CISO, Top 5 US Brokerage

These two statistics show why businesses are stuck between a rock and a hard place:

“…over two-thirds of consumers globally expect brands to protect their interests when using private data. The result in the US was even higher, with 72% of consumers having that expectation.”12

“74% of people are likely to switch brands if they find the purchasing process too difficult.”13

According to Forrester, “The majority (66%) of adults feel that valuing their time is the most important thing a company can do to provide them with good online customer experience.”14 Companies realize that asking too many questions or placing too many time-consuming obstacles—all to establish a customer’s identity—can be seen as not valuing the time of customers.

The three pillars that organizations want to achieve but feel they cannot achieve are customer satisfaction, reduced operational costs, and reduced fraud. Trying to escape the demands of human-staffed call centers through technology is not working. In a blog post, Forrester notes, “To manage ballooning volumes of interactions across an increasing number of channels, customer service teams today increase their staff despite the cost: 46% of global contact center decision makers project their contact centers to grow by 5%-10% in the next year.”15

Despite Forrester cautioning that companies need to reduce this growth through automation and AI, the importance of call centers are not going away any time soon. That means call centers must still deal with satisfying customers, reducing fraud, and keeping call center operational costs low. It may seem like you need to sacrifice one pillar for another, but with the right anti-fraud and authentication solutions, that’s not the case.

PART FOUR:

Fraud Rate by Industry

As call center fraud grows in frequency, sophistication, and methodology, fraudsters also run into technology roadblocks that close channels for them to exploit. They then refine and adjust their schemes, and examine weak points and unique opportunities across industries.

The fraud rate across all industries 2017 saw a 47% increase attributed to data breaches, fraudster leverage multiple channels undetected, over reliance on KBA questions for security, and escalating technology on both sides. However, looking deeper at fraud across multiple industries, it is clear that fraudsters vary how they execute attacks—and these varied attacks also impact organizations differently. The increase in fraud rate by industry shows some interesting trends that don’t necessarily describe the full extent of these unique fraud problems.

<table>
<thead>
<tr>
<th>Industry</th>
<th>YoY Fraud Rate Increase</th>
<th>4 Year Fraud Rate Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insurance</td>
<td>36%</td>
<td>248%*</td>
</tr>
<tr>
<td>Banks</td>
<td>20%</td>
<td>269%</td>
</tr>
<tr>
<td>Retail</td>
<td>15%</td>
<td>134%</td>
</tr>
<tr>
<td>Card Issuers</td>
<td>14%</td>
<td>24%</td>
</tr>
<tr>
<td>Brokerages</td>
<td>4.5%</td>
<td>78%</td>
</tr>
</tbody>
</table>

*Data based on last 3 years

Let’s look at each industry more closely.

INSURANCE

While the insurance industry experiences considerably lower fraud rates than the banking vertical—with much less repeat fraud, an individual fraud incident can be much more costly. Insurance fraud can be more complex than banking fraud. With insurance, a fraud incident usually involves more calls and it takes much more time between the initial reconnaissance and final payout.

That payout can be huge. Transactions can involve tens of thousands, hundreds of thousands, or even millions of dollars. That’s why insurance fraudsters typically make more calls to gather intelligence on intended victims, study the paper trail of their target firm, and take their time before initiating the fraudulent attack. Because of the large potential gains from personal pension plans, 401ks, IRAs, and life insurance policies, fraudsters invest more time here versus a typical smash and grab account takeover.

Unlike brokerages, insurance companies are seeing a much greater rate of increase in voice fraud, increasing 36% from 2016 to 2017 and 248% since 2015.

Fraudsters heavily rely on VoIP for most calls, suggesting that insurance companies may not have enough voice channel security measures in place to flag fraudulent calls. Because of VoIP’s anonymity and ease of use, fraudsters find VoIP a great tool for reconnaissance.
Identifying the calling behavior of fraudsters, such as how many times they have called an insurance provider or how many times they have called other similar institutions, is critical to stopping insurance industry fraud. A fraudster will call many times before attempting a transaction—and when they make that final transaction, it’s often too late to stop at that point.

FRAUDSTER PROFILE

Policy Marm

The Policy Marm phishes through the phone channel to get information about insurance policies and personal pension plans over the course of a week, gains intimate knowledge about the rules and processes involving large withdrawals, and pretends to be an elderly female to gain the trust of call center agents.

Objective: To carefully withdraw a large amount of money but not the entire fund—which would trigger a notification to the account holder.

Weakness: To maintain the ruse that the Policy Marm is, in fact, the policy holder, she must call using the same number each time. Her repeated attempts from the same phone number makes her identifiable.

How to catch her: Intelligence from Pindrop can stop the Policy Marm on her first attempt when she tries to attack multiple organizations. Since she must maintain the same provider and phone number, repeated calls will raise her risk score.

RETAIL

On an absolute basis, the retail industry continues to be hit with the highest fraud rates overall and still experiencing a 15 percent increase in the voice fraud rate from 2016 to 2017. In fact, since 2014 the retail industry fraud rate has increased 134% as more sales take place online, over the phone, and through omni channel processes. For example, the United Kingdom saw an increase of 50% in fraudulent identities used to open cellular telephone accounts, which involved fraudsters using online and call center access accompanied by reshipping techniques to defraud retailers.
Because of its anonymity capabilities and ease of use, VoIP is the most used origin for fraudulent retail calls at 58 percent (although 39 percent of calls do originate from cell phones). 75 percent of fraudulent retail calls come from abroad. In fact, fraudsters have developed sophisticated ways to operate internationally while exploiting unwitting “employees” to help them ship fraudulent purchases to desired countries. The bank accounts funding these operations are also showing growth. In the UK, accounts that were flagged as money mule accounts grew by 11% in 2017 according to a CIFAS fraud study.

44% of Attackers Use VoIP Gateways
Why are call centers such an easy target for these retail fraudsters? Reshipping schemes rely on weak voice channel authentication combined with the high volume of small purchases that retailers transact every day. It’s easy to blend into such transaction noise.

For example, a retailer experiencing a fraud problem might notice many small items fraudulently purchased for resell. While this creates a high fraud rate, the low cost of the items leads to a relatively small fraud exposure. If a fraudster takes over an account and purchases a smartphone, the fraud exposure is just a few hundred dollars. This makes fraud hard to spot and potentially disincentivizes retailers from taking stricter steps to prevent it—despite fraudsters increasingly targeting this industry.

**RESHIPPING SCAM - HOW FRAUDSTERS MOVE THESE STOLEN GOODS OVERSEAS**

Typical Scenario:

1. Fraudster recruits reshippers (Craigslist, email, job websites...)
2. Fraudster places merchandise order (Stolen CC, account takeover)
3. Merchandise shipped to reshipper to avoid international suspicion
4. Reshipping agent receives packages and then sends goods overseas
5. Fraudster receives goods and sells on international market

*Happens FAST, nearly impossible to recover losses, very tough to prosecute!*

Why are call centers such an easy target for these retail fraudsters? Reshipping schemes rely on weak voice channel authentication combined with the high volume of small purchases that retailers transact every day. It’s easy to blend into such transaction noise.

For example, a retailer experiencing a fraud problem might notice many small items fraudulently purchased for resell. While this creates a high fraud rate, the low cost of the items leads to a relatively small fraud exposure. If a fraudster takes over an account and purchases a smartphone, the fraud exposure is just a few hundred dollars. This makes fraud hard to spot and potentially disincentivizes retailers from taking stricter steps to prevent it—despite fraudsters increasingly targeting this industry.

*Oops! I Made a Mistake*

A recent story in Digital Trends reported on various mistakes made by Alexa when interpreting children’s conversations, background conversation, and even a parrot’s talking as a product order. Today, these anecdotes are a source of amusement. Going forward, this vulnerability may become exploited by fraudsters.

As the voice channel grows and involves more endpoints like personal assistants, these endpoints will need better security. With no keyboard, personal assistants must rely on voice biometrics—a traditionally problematic authentication. Opportunity exists to provide better security for this emerging voice channel.
BANKS

For obvious reasons, banks remain a lucrative target for fraudsters despite heavy security. From 2016 to 2017, the fraud rate in the phone channel increased by 20 percent—and an increase of 269% from 2014 to 2017.

This year, Pindrop Labs also began to focus on segmenting out credit unions for observation. In 2017, the fraud rate was 1 fraudulent call for every 1429 calls—about half the rate of banks. It is likely that credit unions are not as targeted as banks, due to their size. This might change as fraudsters reach out across industries to maximize their reach and effectiveness. Most credit union fraudulent calls originate from cell phones. The biggest difference between credit unions and all other industries is that most fraudulent calls are actually domestic in origin (80%).
One of the most unique fraud targets and trends that seems to work differently than all other industries is brokerages. It appears that the slow growth of this industry’s fraud rate (4.5% between 2016 and 2017 and a steady increase of 78% over four years) means brokerages are a less attractive but still profitable target for fraudsters.

While a brokerage or insurance provider might experience fewer fraud calls into its call centers, those few fraud calls target accounts potentially worth millions. This leads to a higher fraud exposure for those fewer calls.

Similar to retail, the majority of brokerage calls stems from VoIP (62%) while a lesser percentage originate from cell phones. Yet, like banking, the balance between international calls (54%) and domestic calls (46%) is more even. The heavy VoIP calls may result from brokerages not yet treating security as seriously as banks. Fraudsters tend to use the calls to brokerages as information collection later used to take over an online account.

### FRAUDSTER PROFILE

**The Tourist**

“The Tourist” calls into credit unions posing as an account holder and informs the call center that he is leaving the country. He requests that they don’t block any foreign transactions.

**Objective:** To grease the wheels at a credit union with social engineering to ensure that unusual activity is not flagged.

**Weakness:** The Tourist fails to get past credit union call centers with authentication and anti-fraud technology in place.

**How to catch him:** Flag his call reputation and stop him on his first attempt. Shared intelligence from the Pindrop Consortium can leverage economies of scale and stop The Tourist in his tracks.

### BROKERAGES

<table>
<thead>
<tr>
<th>Year</th>
<th>Fraud Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>1 in 3000</td>
</tr>
<tr>
<td>2015</td>
<td>1 in 2700</td>
</tr>
<tr>
<td>2016</td>
<td>1 in 1761</td>
</tr>
<tr>
<td>2017</td>
<td>1 in 1686</td>
</tr>
</tbody>
</table>

Similar to retail, the majority of brokerage calls stems from VoIP (62%) while a lesser percentage originate from cell phones. Yet, like banking, the balance between international calls (54%) and domestic calls (46%) is more even. The heavy VoIP calls may result from brokerages not yet treating security as seriously as banks. Fraudsters tend to use the calls to brokerages as information collection later used to take over an online account.
CARD ISSUER

Card issuers have seen a smaller but steady increase in fraud rates of 14% from 2016 to 2017 and just 24% since 2014. While still an obvious target for fraudsters, credit cards have offered few rewards to criminals and often quickly become dead ends. Credit card numbers are sold cheaply on the dark web or encrypted chat apps like telegram because they often don’t work for long. All it takes is one or two anomalous large purchases for a card to get flagged and shut down. However, a lot of credit card fraud still works and can fly under the radar of anti-fraud technology at card issuers, and so this industry will continue to attract fraudsters.
Fraudsters appear almost balanced between using cell phones and VoIP to make fraudulent calls to card issuers. Most card issuer call center fraud originates from international callers.

**UTILITIES**

Like other industries, utility companies fall victim to fraudsters taking advantage of weak customer account processes and poor voice channel security. Unlike banks, utility companies require very little information to create an account—so much so that legitimate customers often have trouble detecting and resolving an account takeover. Fraudsters take their time and slowly exploit these weak points for months and years. Weak access points make their job even easier.

While some fraudsters are simply trying to steal utility services, more sophisticated fraudsters may seek to extract personally identifiable information, or PII, and account credentials. They then use that information to enter more protected accounts at banks and financial services organizations. The phone channel at utility companies becomes just another part of the multi-channel game for fraudsters.

Customer fraud may seem like a necessary evil to utility companies, but it’s harder for them to shrug off data breaches and threats to national security stemming from the phone channel. According to a Ponemon Institute study (sponsored by IBM), data breach incidents averaged a cost of $7.4 million for US utility and energy companies.\(^{18}\) Fraud and theft in the utilities sectors cost Europeans companies around €3.7 billion each year.\(^{19}\)
And beyond financial damage, the ease of creating fake utility accounts and taking over customer accounts are symptoms of a weak security link in US critical infrastructure that fraudsters and even nation states may exploit to steal more significant data and even shut down utilities.

Russia is an example of a nation state successfully hacking private utility companies during the last two years by exploiting security weaknesses. In March 2018, the Department of Homeland Security (DHS) published an alert\(^\text{20}\) that reported on “a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities’ networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS).”

Within the alert, we see basic key fraudster techniques such as credential gathering and spear phishing, which make call centers with weak authentication practices especially vulnerable. When authentication controls are not in place and strong at an access point like the phone channel, utility call centers become vulnerable during nation state reconnaissance. They can even become a secondary cyberattack target used by an adversary to hamper recovery after a major incident (such as shutting down a power grid). During an attack in December 2015 that shut off power for more than 200,000 Ukrainian customers, Russia “carried out a denial of service attack against one company’s call center, flooding it with fake calls to stop company personnel from identifying the blackout area.”\(^\text{21}\)

Utility companies must take phone channel security more seriously not just to protect customers but also to prevent data breaches and critical infrastructure attacks that potentially affect national security.

HEALTHCARE

As fraudsters grow more sophisticated, they target industries with higher payoffs. One such higher payoff is achieved with the theft of healthcare records, information, and data. On the black market, healthcare records often earn criminals ten times more than a credit card number. Healthcare records are also valuable when fraudsters want to steal even more money by submitting false claims, receiving prescription drugs, or even purchasing medical equipment.

In 2017, healthcare providers experienced 23.7% of all data breaches and remained the second most targeted industry sector.\(^\text{22}\) Healthcare identity theft also increased by 21 percent last year.\(^\text{23}\) But despite these intense cyberattacks, the healthcare industry continues to lag other industries in implementing cybersecurity best practices and securing the voice channel.

The impact of weak healthcare security devastates victims who often must pay an average of $13,500\(^\text{24}\) after an incident and take many, many hours to resolve the issue. When fraudsters steal medical information, victims may also suffer consequences such as changed medical records (leading to doctors misdiagnosing or misprescribing, which endangers that person’s life), legal troubles, and even loss of health insurance.

\(^\text{20}\)https://www.us-cert.gov/ncas/alerts/TA18-074A
\(^\text{22}\)2017 Annual Data Breach Year-End Review, (2018), idtheftcenter.org/2017-data-breaches/
Financially, fraud hits healthcare hard. The cost of fraud to the healthcare industry falls somewhere between $80 billion and $200 billion each year with a low recovery rate (about 5 percent) that burdens healthcare providers, insurers, and consumers. With such success for fraudsters, it’s easy to see why they take aim at healthcare organizations—and especially call centers where authentication and security is weak.

Some fraudsters are experts in multichannel attacks that even exploit offsite locations such as medical clinics and health fairs where low security health screenings take place. There, they capture valuable information about victims. Medical personnel in on the scheme may share information with fraudsters who then use that information to access further medical information on the phone channel.

It’s important that healthcare providers ramp up security overall, and they can shore up a significant weak link by better securing the phone channel. Implementing better anti-fraud and authentication procedures in the call center can help make healthcare providers a harder, more frustrating target instead presenting itself as such a lucrative industry to attack.

PART FIVE: Looking Ahead

Because of AI and automation, many people have the impression that we won’t have a need for call centers in the future and that the voice channel may become a thing of the past.

Actually, our full immersion into the voice channel may be just getting started.

While most voice channel technology has focused primarily on the call center, we are seeing massive growth in digital assistants on our smartphones, tablets, computers, and standalone devices in our homes. These digital assistants will extend to our cars, our appliances, and to anything in the future with an internet connection. And for each digital assistant, there is a potential for fraud, hacking, and security exploits.

Plus, the rise of omnichannel makes human interaction still valuable and demanded. People want to go to stores and talk to humans who solve their problems. That need for human interaction still leads companies to staff call centers with agents who provide customized service. Omnichannel puts control in the hands of customers—and that includes all service options such as the voice channel.

“The proliferation of voice technologies will continue to put consumers’ security and identity at risk. Currently, fraudsters can easily get around existing authentication methods. As businesses adopt the latest voice technologies for the majority of customer interactions, there will be a parallel need for top-notch security.”

-Vijay Balasubramaniyan, CEO and Cofounder, Pindrop

How will companies handle omnichannel security as this paradigm becomes a priority? By just focusing online but not on voice? Sadly, that is the case today as companies largely neglect the voice channel. Poor customer experience results from this neglect, and this poor customer service costs businesses money, customers, and even data (from data breaches).

A recent Pindrop report\(^\text{27}\) states:

Pindrop also found that more than two-thirds of businesses are planning to use voice assistants like Amazon Alexa and Microsoft Cortana for the majority of customer interactions, and nearly one in four plan to use them for all customer interactions. Voice technology is an important driver of customer satisfaction according to 94 percent of managers, and 88 percent believe it will give them a moderate or strong competitive advantage. Voice technology will increase operational efficiency according to 57 percent, and the same number believe it will reduce the cost of each customer transaction.

And...“U.S. businesses are leading the adoption of voice technologies, as they are 10 percent more likely to use them now, and 15 percent more likely to believe chatbots or voice-activated assistants will handle the majority of customer interactions in the next five years. More U.S. businesses also think voice technology will give them a competitive boost, by 11 percent.”

---

So, businesses are going to rely on digital assistants for increasing customer experience, gaining a competitive edge, and increasing operational efficiency. But all these gains are lost if security is not factored into the equation. The Pindrop report states that “security is a significant concern, however, for 90 percent of U.S. companies, and 80 percent of global companies overall.”

As we’ve seen, fraud rates are increasing overall and at different rates for various industries. Each industry has its own unique challenges related to fraud. The trends show that call centers are not going away and that we will rely on the voice channel—both with human agents and digital assistant technology—more than ever. Yet, voice channel security remains our weakest link in the security industry.

That needs to change. Hopefully, this fraud report highlights the growing issue, that it’s not going away, and that we need to be proactive, innovative, and creative in solving these problems to not only defeat fraudsters but to also make sure our businesses remain secure for our customers’ sake.