The Weakest Link

Public Sector Phone Channel Security

Weak phone security sabotages and jeopardizes all other information security efforts. The root cause of fraud loss, the call center, is often misdiagnosed.

Introduction

In early 2016, a hacker published the names and personal details of approximately 20,000 FBI employees and 9,000 Department of Homeland Security employees after collecting the information through a Department of Justice employee's email account. The hacker began by obtaining the employee's email credentials. However, when he attempted to log into the Department of Justice's web portal, he couldn't proceed without a token code. Calling the department's helpdesk, the hacker acted the part of a new employee. The helpdesk agent, aiming to provide painless customer service, provided the necessary token code and granted the hacker access to the confidential data.[1]

These massive data breaches lessen public trust. Financial security and personal privacy are heavily impacted when data breaches leak an individual's confidential, hard-to-replace information, such as Social Security numbers, tax ID numbers, and Medicare IDs. Financial loss, public outrage, and government investigations often follow.

Regulators in the information security industry have collaborated to address critical physical and online information security gaps through strengthened regulations, technologies, and recommended best practices. However, the phone channel, which is traditionally perceived as an isolated and less important part of information security, now attracts fraudsters as an access point. These fraudsters use the information they gain from the phone channel to bypass security measures in physical and online channels.

Effective information security involves a tightly interwoven combination of physical, online, and phone security. Sixty-one percent of fraud can be traced back to the call center.[2] However, fraud is a cross-channel problem. Each channel impacts the other, and the law of the weakest link applies. Weak phone security sabotages and jeopardizes all other information security efforts. The root cause of fraud loss, the call center, is often misdiagnosed.

1. Hacker Plans to Dump Alleged Details of 20,000 FBI, 9,000 DHS Employees." Motherboard.February 7, 2016.

2."Contact Centers: The Fraud Enablement Channel." Aite Group, 2016.

The Failure of the Legacy Solutions in the Phone Channel

Traditional call center anti-fraud and authentication methods no longer stand up to the advanced tactics leveraged by today's fraudsters. Most call centers heavily rely on Caller ID and knowledge-based authentication (KBA) that fraudsters easily workarounds for fraudsters. Caller ID information can be easily spoofed. According to Gartner's Avivah Litan, VP Distinguished Analyst, KBA (asking questions that only legitimate callers can supposedly answer) has an average failure rate of 10-15%, and this rate can sometimes go as high as 30%. Most of these failures come from legitimate callers, not fraudsters. Meanwhile, over 60% of these fraudsters can successfully answer these questions because of data they've already stolen.

Organizations train their customer service representatives to look for red flags and calls originating from specific areas of the world. However, compared to the security layers that protect physical information such as ID, surveillance, or chip cards, and online information security such as login protocols, IP addresses, or session monitoring, legacy solutions fail to provide the multi- layered solution necessary to successfully combat fraud.

Security in the public sector call center should provide:

- Universal Coverage: Phone security needs to protect every incoming call by authenticating trusted callers and identifying fraudsters on their first call.
- Accuracy: Phone security needs to catch fraudsters without triggering false negatives about legitimate callers. Caller ID and KBA verification don't meet this level of accuracy.
- Speed: Phone security needs to ensure that call center agents are informed about the legitimacy of callers before they allow access to accounts and personal data. KBA- based solutions take too long, which frustrates legitimate callers and offers fraudsters many chances to collect data.
- Low Friction: Phone security fails if it ruins the customer experience. A solution shouldn't add extra steps to an interaction.
- Fraud-Resistant Technology: Phone security must withstand attempts by fraud rings to overcome existing protections. Everything on the market today—Caller ID, KBA, and voice biometrics—fails to combat voice distortion, spoofing, social engineering, gateway hacking, and other tactics used by fraudsters to circumvent security measures.

Exploiting Cross-channel Weaknesses Through Social

Finding it easy to fool call center agents through social engineering, fraudsters increasingly use psychology, behavioral knowledge, and acting to convince and persuade others to give up information. Phishing by phone (also known as "vishing") works by the same principles as online phishing—persuading a call center agent to reveal personal, sensitive, and/or confidential information about citizens, employees, or the government.

In the public sector, public trust is of the highest value. Phone fraud is not isolated from online cyber security crime. Fraudsters often collect information by phone to help with their physical and online attacks—and vice versa. For example, a fraudster may first collect personal information about a citizen from a social media platform. He can then use that information to impersonate his target, engage with a call center employee, and attain a password needed to accessan account.

The Authentication Problem

At its core, security relies on authentication. To access certain data, you have to know something (like a password), have something (like a token), and/or be something (like a specific fingerprint). Layered authentication leads to stronger security.

Over the last few years, the government has increasingly recognized the importance of multi-factor authentication for cybersecurity. At the federal level, recent efforts by the Office of Management and Budget (OMB), National Security Council (NSC), and Department of Homeland Security (DHS) have addressed authentication by focusing on the use of personal identity verification (PIV) cards, increasing strong authentication around privileged users, and making sure mobile devices are locked down. However, a focus on phone channel vulnerabilities is still missing from these efforts.

The Pindrop® Multifcator Analysis Engine

To combat these existing vulnerabilities, Pindrop addresses the security layers that traditional phone channel security lacks with the Pindrop® anti-fraud solution. A combination of metadata, PhoneprintingTM technology, and voice biometrics helps relieve the

Metadata

For each phone call, Pindrop has developed a methodology to immediately examine a phone number's calling history against the Pindrop NetworkTM technology, which includes:

• The Pindrop® Consortium.

With data collected on over 500 million annual calls, the Pindrop NetworkTM technology provides a wealth of information about these phone numbers, including previous fraudulent activity.

• Telecommunications Data.

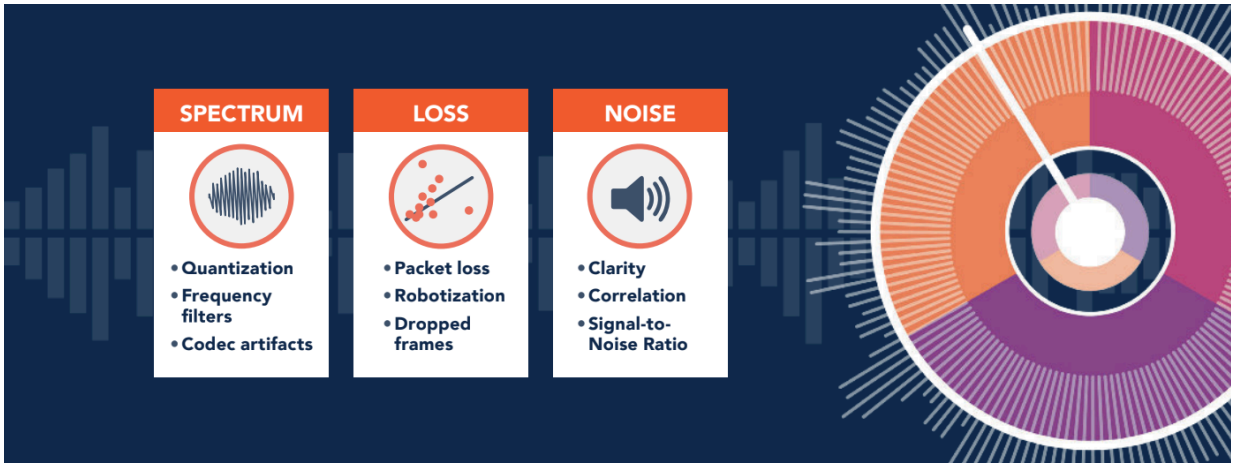
This data provides crucial information including the number's origin, device (VoIP, landline, cell), and carrier. When this information doesn't match up with previously recorded data, it's a big red flag.

• Research.

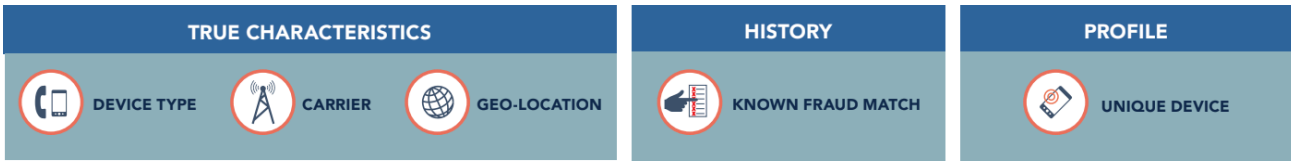
Pindrop collects information about consumer complaints and the FTC's Do Not Call Registry while also conducting its own research. In addition, the Pindrop® Phoneypot tool, a large-scale telephony honeypot, measures attacks and detects calling patterns for unwanted callers.

Pindrop addresses the security layers that traditional phone channel security lacks...

147 Factors are analyzed to create a distinctive telephony signature



PhoneprintingTM Results



Phoneprintingtm Technology

Pindrop® PhoneprintingTM technology analyzes the complete audio content of a call rather than just voice. This patented technology isolates and examines 147 characteristics of each call to determine the unique phone device, type of call (VoIP, mobile, landline), and approximate geographic region from which the call originates.

By comparing the phone device, call type, and geographic location with the call information reported by the Caller ID and phone network, the PhoneprintingTM technology can detect Caller ID spoofing attempts. For example, if the Caller ID metadata indicates the call is coming from a landline in Atlanta, Georgia, but the audio reveals the call to riginate from a VoIP phone in Nigeria, the caller is likely a fraudster.

Phoneprintingtm Technology

Voiceprints are taken for that caller and used to identify him in the future. Pindrop® technology detects fraudsters by anomaly when they first call. After that, a voice biometrics blacklist helps quickly detect the same fraudulent caller in the future.

Tying it all together

Pindrop's solution combines data from these three complementary technologies to create a risk score that's easy for call center agents to see and act upon within seconds. In near real time, the Pindrop® anti-fraud solution sends the risk score accompanied by a red or green light. A red light allows agents to stop a fraudster's efforts before accidentally granting access to personal data, and a green light ensures that legitimate callers receive prompt service. This risk score is available any time afterward for fraud analysts to investigate in the Pindrop® Case Manager tool, where they can create profiles of known fraudsters.

About Pindrop

Pindrop is the pioneer in voice security and authentication. Pindrop provides enterprise solutions to reduce fraud losses and authentication expense for some of the largest call centers in the world. Pindrop's patented PhoneprintingTM technology helps identify, locate and authenticate phone devices uniquely from the call audio, thereby detecting fraudulent calls as well as verifying legitimate callers. Pindrop has been selected by the world's largest banks, insurers, brokerages and retailers,detecting over 80 percent of fraud. Pindrop® solutions are allowing customers to reduce call time and improve their customer's experience even while reducing fraud losses. Pindrop was founded in 2011 and is venture backed by Andreessen Horowitz, CapitalG, Citi Ventures, Felicis Ventures, GV and IVP.

Fitting contact center security into your public cybersecurity info

The Pindrop® methodology and approach offers a comprehensive anti-fraud and authentication solution that surpasses the limitations of Caller ID, KBA, and voice biometrics by combating a fraudster's methods with a strong form of fraud detection, independent of anything they can socially engineer or control.

However, call center security forms only part of an overall information security plan. For example, Carahsoft now includes the Pindrop® anti-fraud solution as part of its go-to suite of cybersecurity solutions for federal, state, and local government. Carahsoft specifically matches its portfolio of cybersecurity solutions with the NIST Cybersecurity Framework, which is based on the White House's executive order for Improving Critical Infrastructure Cybersecurity.

By including Pindrop® technology in its portfolio of threat detection solutions, Carahsoft complements its other security efforts. Governments can now more quickly adapt the Pindrop® solution as part of Carahsoft's GSA schedule.

By not addressing weak points, government agencies run the risk of diminishing the success of their other cybersecurity efforts and potentially increasing the risk of serious consequences such as citizen data breaches. These breaches may affect the public's trust. Using the Pindrop® anti-fraud solution might help bolster the weak points in your call center and your cybersecurity plan.