PROTECTING YOUR CALL CENTERS AGAINST PHONE FRAUD & SOCIAL ENGINEERING

A WHITEPAPER BY PINDROP SECURITY
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>The Evolution of Bank Theft</td>
<td>4</td>
</tr>
<tr>
<td>Phone Channel Vulnerabilities</td>
<td>4</td>
</tr>
<tr>
<td>Financial Institution Fraud Attacks</td>
<td>5</td>
</tr>
<tr>
<td>Defenses</td>
<td>7</td>
</tr>
<tr>
<td>Pindrop Security Technology</td>
<td>8</td>
</tr>
<tr>
<td>The Pindrop Ecosystem</td>
<td>9</td>
</tr>
<tr>
<td>Accuracy</td>
<td>10</td>
</tr>
<tr>
<td>Pindrop Solutions</td>
<td>10</td>
</tr>
<tr>
<td>Fraud Detection System</td>
<td>11</td>
</tr>
<tr>
<td>Phone Reputation Service</td>
<td>11</td>
</tr>
<tr>
<td>Phone Fraud Assessment</td>
<td>12</td>
</tr>
<tr>
<td>Call Forward Protection</td>
<td>13</td>
</tr>
<tr>
<td>About Pindrop Security</td>
<td>14</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Phone fraud is a growing problem for financial institutions due to its ease, low risk and low cost. It comes in many forms with attacks in the call center, in automated account management systems, and outbound verification systems. It costs financial institutions in terms of losses, call center time and expense and incident response. It also erodes trust with customers.

This paper will explore the costs and issues around phone fraud and then explore a solution that can alleviate this issue for institutions.
Phone attacks against financial institutions (and anyone else with a call center or toll free number) are increasing rapidly, with the first half of 2013 seeing almost as many attacks as all of the prior year\(^1\). Why? As opposed to physically robbing a bank or hacking into the network, the phone channel is quite vulnerable, with little defense in place.

**Phone Channel Vulnerabilities**

The phone system presents a perfect storm of characteristics, both new and old, that invite malicious abuse.

**Caller ID is broken** – Caller ID (CID) and Automatic Number Identification (ANI), two systems designed to provide information on callers, actually have no security built-in or available. They originally were designed to be used internally by the phone companies – no security needed. The result is that spoofing Caller ID data is very easy – for instance, one smartphone app, Caller ID Faker, has over 1,000,000 downloads. The app even includes voice-masking features. One person's practical joke app is another person's fraud tool.

**It's cheap and easy** – With the rapid spread in VoIP networks beginning in the 1990's, the world of telecommunication has changed significantly. The cost of long distance calls has fallen drastically, making it practical to call the US from anywhere in the world cheaply. VoIP allows wide use of PC applications to perform a wide range of activities, many beyond the scope or intent of the phone network. This includes automated dialing and easy-to-use spoofing technology.

---

1 Pindrop Security, State of Phone Fraud Report
No metadata – Every phone call traverses multiple networks, no two of which is exactly alike. In fact, even if you use your cell to call your landline while standing next to your home phone, you’re using at least two networks. Since phone networks are also very bad at sharing information with each other about the call, the only data to get through every network the call traverses is the actual call audio. There is no data shared that provides caller verification or origination. And even call audio suffers degradation – we’ve all experienced poor quality calls. The recipient of a phone call cannot count on any information about the caller coming through intact.

Financial Institution Fraud Attacks

Total bank fraud losses are around $4 billion per year and it’s estimated that from 30% to 50% of fraud incidents is initiated with a phone call1. Phone fraud is also frequently combined with online and in-person fraud, particularly to gather information or escalate privilege prior to the actual fund transfer attack. The main problem areas for financial institutions are:

Call centers

Talking to a call center representative presents a fraudster with several advantages. First, fraudsters are typically professional social engineers – they are experts at manipulating people. Second, call center representatives rightfully prioritize being helpful – they want the customer to get the password right or successfully complete the transaction. Third, despite the overall fraud call volume being high, the average call center representative will only be dealing with a fraudster once in approximately every 2000 calls. Identifying and handling a fraudster is not a core competency for that rep.

Once on the phone, the fraudster may attempt a direct attack, stealing funds via a wire transfer. They may request a rush or replacement card and then max out the card with purchases. If they don’t have all the credentials or access they need, they may opt to take more innocuous steps in order to set up a future attack. A change to the address, phone number or email allows them to transfer the point of contact to an asset they “own”. They can claim to be a customer who will be traveling overseas (known as “travel strategy modification”) resulting in lower fraud alerting levels at the bank.

2 Identity Theft Tops FTC Complaints in 2011
The only defense against these fraudsters is the asking of a few personal questions (known as knowledge-based authentication or KBA). If a fraudster can provide that information, the ability to move funds is practically unrestricted.

**Automated phone systems**

Fraudsters can also steal from you and your customers without talking to a representative. Automated systems or IVR's (interactive voice response) systems allow a wide range of account activities that allow a fraudster to make substantial inroads to taking over an account. As with a live rep, getting an account address, email or phone number changed can allow a fraudster to order a replacement credit or debit card and then clean funds out of an account. And they only need access to the account for a few hours prior to detection to be successful. In addition, fraudsters will check account balances on accounts to identify high value targets.

Even high dollar transactions can be completed using automated systems and the website but with an additional out-of-band step for verification. Typically, this is a phone call to the number registered to the account that asks for a code provided by the website to be entered. The weakness in this system is if the registered phone number has been forwarded or otherwise redirected to a different number.

**New accounts**

Many fraud schemes require a legitimate account at the targeted bank. These include both phone-based and online attacks. When accounts are set up, the fraudster will likely use a real phone number as it may be required to verify the account owner. These accounts are lurking in banks now. They took time and money to set up and they are ready to be used to support fraud schemes.

**After-action incident response and forensics**

When fraud has occurred or is suspected, fraud teams go into action. Most phone fraud investigations, whether formal or informal, start by looking up the phone number in a search engine, number lookup site or official records database.

None of these sources is particularly helpful - the information available is inconsistent and anecdotal. From there, analysts may need to call the number or contact third parties such as telco's. Again, results tend to be unsatisfying and the process is time-consuming, expensive and frustrating.
Telecommunication costs

A novel attack that is impacting financial institutions and other industries that combine toll-free numbers with extensive automation of call systems, traffic pumping costs banks money for non-business calls. Specifically, calls are made to a bank's automated, toll-free line and then continued through maximization of pauses and automatic transfers, to use as much time as possible before a live agent finally realizes the call is bogus and terminates. The local exchange carrier that originated the call is entitled to intercarrier transfer fees from the bank's telecommunication provider, which, in turn, is charging the bank. Typically, the local exchange carrier has commissioned the attack.

There are many points of vulnerability. What can be done to protect them?

Defenses

We're all familiar with the leading deterrent to phone fraud - companies grill customers with questions. Knowledge-based authentication (KBA), examples include asking for your mother’s maiden name, high school mascot, pet’s name. It's not very sophisticated, it's very expensive (in excess of $10 billion a year) and it's not very effective. Not only are many of the answers easy to guess or bluff but call center reps - who are focused first on customer service - actively help callers answer the questions correctly.

A variety of technologies have been developed to address this problem. Analyzing the caller’s voice, which is known as voice biometrics, focuses on authenticating callers to detect known bad actors and to positively identify bank customers. This is useful for authentication of customers but not for detecting fraud. Call verification tries to confirm if the caller is who they claim to be using call signaling information.

This method is highly inconsistent, depending heavily on the originating callers provider network and device type. While each of these methods has value, as stand-alone solutions their value doesn't justify the cost of deployment. Combined, they start to add up to an answer to the problem.
A Viable Solution

In order to justify the time and cost of deployment, a solution would need to be able to do the following:

• Identify new attackers before they can do damage.

• Identify attackers in all parts of the phone infrastructure: live calls, recorded calls, automated answering systems and outbound calling systems.

• Use both phone number or call audio to identify and quantify fraud risk.

PINDROP SECURITY TECHNOLOGY

At Pindrop Security, our mission is to restore trust in the phone channel by providing a set of solutions that deliver the protections we've outlined above.

The Pindrop Fraud Detection System (FDS) is designed to analyze all aspects of the call to detect indicators of fraud. We are able to identify tactics such as Caller ID spoofing, voice distortion and autodialers. We track reputation including high volume callers, association with fraud rings, and past fraud. And we track callers, both good and bad, across the globe.

At the core of Pindrop is a unique technology called “phoneprinting™” which analyzes the audio content of the call itself. Phoneprinting isolates and analyzes 147 characteristics of each call and, from this, determine the caller’s geography and the calling device type and therefore identify spoofing. At our customer sites, phoneprinting alone reveals over 80% of fraud calls immediately upon receipt of the first call.

In addition, Pindrop Security’s technology creates a unique fingerprint tied to the call. This fingerprint will identify a fraudster (or legitimate customer) regardless if the voice is manipulated, the number is changed or spoofed, or even if the caller is changed (as in a fraud ring or fraud call center). No other solution can do this.
About Phoneprinting™

The phoneprint is the key to Pindrop Security’s solutions. By analyzing less than 20 seconds of audio, we can match the fingerprint and identify fraudsters. Or, if all you have is a phone number, we can identify if that number has ever been attached to a suspicious fingerprint.

What Does a Phoneprint Tell You?

**Spoofed Call**  The caller is hiding their true number or impersonating another person

**True Location**  Where the call is really coming from?

**True Device Type**  Whether the caller is using a Cell, Landline or VoIP to place the call? If VoIP, which network?

**Recognized Caller**  Has the caller been seen before?
Phoneprinting™ Accuracy

Pindrop’s phoneprint technology is highly accurate. It is able to determine the location of the caller and the type of device being used to originate the call (VoIP, Cell, Land) – even the network type for VoIP calls (Skype, etc.) with over 90% accuracy. While this information alone is enough to determine fraud, we go further by then matching the fingerprint to our database of fraud rings and repeat fraudsters. Typically, a fraudster will have a large number of phone numbers and will have targeted many institutions. This information is made available as well, to assist fraud and incident response teams. Our fingerprint matching is over 99% accurate.

About The Pindrop Consortium

The Pindrop Consortium feeds our phone number and caller reputation database. The Consortium leverages information from our enterprise customer calls, consumer call data and specialized monitoring systems developed by Pindrop. The result is reputation information based on millions of calls and phone numbers available in real-time to protect your enterprise.
PINDROP SOLUTIONS

Pindrop offers several solutions; each designed to address specific fraud risk areas within financial institutions. Together, they provide a complimentary and complete solution for financial institution phone fraud.

Fraud Detection System

Pindrop Security’s Fraud Detection System (FDS) analyzes phone calls to identify fraudulent callers. FDS analyzes live or recorded call audio to identify call spoofing and other indicators of fraud by providing a highly accurate call risk score. It verifies location and call type and matches it against Caller ID or ANI data to identify spoofing. It also creates a unique fingerprint for the caller and compares the fingerprint to our database of known fraud rings and repeat fraudsters regardless of the real or spoofed number they are using (VoIP, Cell, Land) – even the network type for VoIP calls (Skype, etc.) with over 90% accuracy.

But phoneprints are not the only tool in the Fraud Detection System. In addition, FDS includes the following technologies:

- **Voice biometrics** are used to track unique individuals for both blacklisting and whitelisting purposes.

- **Reputation** provides real-time updates on the behavior of the phone number and the caller, including call volume, past fraud or suspicious activity, complaints and association with risky networks, devices, callers and locales. This data is gathered from our consortium of customers and partners as well as tracking of robo-dialers and automated calling systems.

What Does FDS Provide?

- Call analysis technology that can determine the actual location and device type used by a caller and compare it to Caller ID or ANI information to determine spoofing and fraud.

- Unique call fingerprint that allows you to match the caller to other fraud attempts and examine their fraud history.

- Non-intrusive validation of customers through transparent location and device type verification.
How Do Financial Institutions Use FDS?

FDS is deployed widely across financial institutions to address a variety of problems. It is used by call centers, fraud investigators, incident response teams and automated systems, to quickly evaluate callers as part of their anti-fraud and transaction approval processes. FDS finds fraudsters already active in your account-base, as well as both known and unknown fraudsters at first contact – blocking them before they ever consume your time or resources, let alone steal from you. FDS also allows financial institutions to reduce the burden of proving identity on their customers while improving their prevention of fraud through identification of deception techniques such as call spoofing.
Phone Reputation Service

For situations in which call audio is not available, we offer Pindrop Security's Phone Reputation Service (PRS), the world’s largest and most accurate database of fraudulent phone numbers.

PRS assigns a unique risk score to every number and provides detailed information, including geography, phone type, and, if a fraud number, specific institutions targeted, attack frequency and other numbers used by the attacking entity. The PRS is either accessed via a web-based interface or directly integrated into your application via an API. PRS displays fraud activities and trends, provides actionable intelligence on suspect numbers, and allows the creation of fraud alerts.

What Does PRS Provide?

- Access to the largest, most comprehensive phone number database with geographic locations, network providers, phone types and any fraud activity history.
- Aggregated intelligence from our phone honeypots (“phoneypots”), email spam traps and complaint collectors as well as intelligence from our customer base.
- Configurable alerting on numbers that are currently targeting enterprises or their customers.

How Do Financial Institutions Use PRS?

PRS is used in several ways by financial institutions:

- **Block unwanted calls** by detecting spam numbers and blocking.
- **Detect attacks on customers** by proactively identifying numbers that are impersonating the enterprise and calling their customers.
- **Investigate incidents** by running phone numbers and analyzing calls associated with an incident.
- **Verify new customers** by checking risk score on provided numbers.
- **Detect future attacks** by checking phone number changes in existing accounts.
Pindrop Security, headquartered in Atlanta, Ga., is a privately-held company that provides enterprise solutions that help prevent phone-based fraud. Its breakthrough phoneprinting technology can identify phone devices uniquely just from the call audio thereby detecting fraudulent calls as well as authenticating legitimate callers. We have helped enterprises eliminate financial losses and reduce operational costs on their phone channel. Pindrop’s customers include two of the top five banks and one of the leading online brokerages. Named SC Magazine 2013 Rookie Security Company of the Year, a Gartner “Cool Vendor” in Enterprise Unified Communications and Network Services, Pindrop Security’s solutions restore enterprises’ confidence in the security of phone-based transactions.