EXECUTIVE SUMMARY

From financial institutions to retailers, the call centre is now the weakest point of entry for fraud activity. In the last year, data collected at Pindrop® Labs has shown a significant increase in the amount of money organisations are losing to phone fraud. In the U.K., £0.86 per call is lost to phone fraud—an increase from £0.51 in 2015.¹ There are more fraud calls than ever, and the sophistication of the criminals behind these efforts continues to grow. One of the main drivers behind the relentless rise in call centre fraud is that attackers are getting better at their craft, honing their skills, and becoming more adept at social engineering techniques that help them bypass call centre defenses.

INTRODUCTION

The call centre is the softest target for fraud in virtually every organisation. Call centre defenses usually only amount to one thing: the call centre agent. Training for call centre employees is designed around providing excellent customer service and not fraud detection.

Fraudsters know this and target their operations at the call centre—what they see as the weakest link in these organisations’ security. In fact, 61% of fraud losses from account takeovers involve the call centre.² By the time a fraudster gets to the call centre, they have often already worked to gather intelligence about the target account and are prepared to strike.

From a data set of more than half a billion calls, Pindrop® Labs reviewed phone fraud activity affecting a variety of industries in the U.K. and U.S. between 2016 and 2017.

SCOPING TECHNIQUES AND THE EXTENT OF THE PROBLEM

To understand the true extent of the problem, it’s crucial to review all call centre interactions between a criminal and a call centre agent. Though many of these calls involve criminals attempting to complete a fraudulent transaction, the majority of fraudulent calls do not involve such a transaction. Pindrop® Labs research shows that a criminal makes an average of five calls before completing a fraudulent transaction. This scoping technique is employed for a variety of reasons, such as resetting passwords, changing mailing addresses, and making other account modifications. In some cases, fraudsters know that their previous activities have caused the organisation to flag their target for fraud, restricting what can be done on the account. Therefore, fraudsters will call again in an effort to influence customer service agents to remove that flag.

Financial institutions, insurance companies, and other frequent fraud targets have invested heavily in securing their online channels in recent years, making online fraud much more difficult and risky for criminals.

¹. Unless otherwise noted, all data and findings come from Pindrop® Labs annual Call Center Fraud Reports, 2013-2016.
². Contact Centers: The Fraud Enablement Channel, Aite Group, April 2016
KEY WEAKNESSES IN THE CALL CENTRE

TECHNICAL
Fraudsters have the ability to spoof caller ID and disguise their voices with easily available technology. They use applications such as Skype or Google Voice to hide their identity and location. Caller ID and location data are now no better or more reliable than an IP address for authentication. Fraudsters also abuse IVR (Interactive Voice Recognition) systems to reset victims’ PINs or find more information about a target.

HUMAN
The real target of call centre fraud attacks is the employee on the other end of the line. Taking hundreds or thousands of legitimate calls for every “bad” call, call centre agents focus on efficiently resolving customer issues and not on filtering out fraudulent calls. The risk of falling prey to a fraudster is high and so is the potential downside if an agent mistakes a legitimate customer for a fraudster.

ORGANISATIONAL
Call centres are designed to efficiently handle huge volumes of activity. Agents are measured on how quickly they resolve each call. Fraudsters use data they’ve gathered about a target account to pass knowledge-based authentication and socially engineer the agent into giving them account access. They will often pretend to be in a rush, angry, or traveling in a foreign country in order to gain sympathy and quickly move the call along.

THE CALLS ARE COMING FROM INSIDE THE HOUSE
While the lack of defenses in the call centre helps enable phone fraud, the phone network itself also plays a part. Simple, freely available tools such as caller ID spoofing apps and voice distortion software allow criminals to circumvent the limited protections that exist on the public phone network. Combined with access to free VoIP software or cheap mobile phones, these tools give even unsophisticated attackers a considerable arsenal with which to work.

Fraud rings are known to spoof caller ID signals to make their calls appear as though they’re coming from inside a target organisation, making their attacks seem legitimate and authentic. In one case, fraudsters would call a large financial organisation saying that they had found a customer’s card, which the organisation would then cancel. Knowing that the customer would soon be alerted by the organisation about the cancellation, the fraudsters would call the customer immediately and impersonate the card issuer. They would use the call to gather personal information from the customer, which the fraudsters then used to call the card issuer back and have a new card sent to them.

FRAUD TOOLS & TACTICS
Cheap infrastructure allows fraudsters to call anyone, anywhere. VoIP software and mobile phones make it cheap or even free. Within the U.K., landlines are rarely used. They make up only 12% of fraud calls. The remaining 88% of fraud calls are split between mobile (56%) and VoIP (32%). The ubiquity and low cost of mobile phones and VoIP software, and the spoofing tools used with them, make phone fraud simple for even low-resourced fraudsters.

Although some scammers tend to stay within their country’s borders, others are increasingly branching out and attacking organisations across international lines. Pindrop® Labs is seeing the emergence of global fraud gangs with 52% of fraud calls originating outside the U.K.

U.K. FRAUDSTER WEAPONS OF CHOICE

- FRAUD CALLS FROM MOBILE: 56%
- FRAUD CALLS FROM VOIP: 32%
- FRAUD CALLS FROM LANDLINES: 12%

pindrop.com | +44-20-3786-4170
This is a clear departure from past years when the vast majority of such calls were domestic. It follows the trend of what’s been happening in the U.S. where 83% of fraudulent calls were from international callers.

Some of these trends can be attributed to the growing problem of phone fraud as an international crime. But it’s also an indication of scammers becoming more confident as they improve their skills and feel competent enough to target organisations in other countries.

The ubiquity and low cost of mobile phones and VoIP software, and the spoofing tools used with them, make phone fraud simple for even low-resourced fraudsters.

This branching out across international lines also presents more opportunities for profit. The average loss per call in the U.K. jumped up to £0.86 in 2016, a sharp increase from £0.51 per call in 2015. As fraudsters improve their skills and gain more confidence in their abilities, they also tend to target higher-value accounts, leading to higher average losses for victimised organisations.

**PHONE FRAUD IN THE NEWS**

**INTERNATIONAL RELATIONS**

In October 2016, three weeks after authorities in India disrupted a major phone fraud ring in Mumbai, the U.S. Department of Justice indicted 61 people in relation to the scam. Officials say it generated as much as $150,000 per day. The indictments are the result of investigations involving U.S. and Indian authorities. According to the U.S. Justice Department, the phone fraud scheme affected tens of thousands of victims all over the world. Twenty suspects were arrested in connection with the case, and five call centres and 32 people in India were also charged. Although this operation targeted consumers, these organised fraud networks are also known to go after call centres in banks and other financial institutions.  

**FRAUDULENT FRAUD DETECTION**

In June, authorities in the U.K. sentenced seven people to prison for their part in running a wide-ranging phone fraud scam that cost victims more than £1.3 million over the course of several years. The scheme that the gang ran is a common and highly successful one that involves making calls to potential victims and telling them that their bank accounts have been compromised. The fraudsters then convince the victims that they need to transfer their money out of the “compromised” accounts and into accounts controlled by the criminals at other banks.

---

3. Dennis Fisher, “IRS Phone Fraud Ring Disrupted in India” OnTheWire.io, October 2016
PROLIFIC U.K. FRAUDSTERS

The Mule
This fraudster opens a large number of savings accounts using different—and very likely stolen—identities. Then, these accounts are used as mule accounts for activities such as money laundering and cheque fraud. The phone channel appears to be the key to attacking these accounts. While some of this behaviour was captured by existing security systems, Pindrop® Labs discovered several currently active mule accounts.

Nomadic Couple
As gentle and soft-spoken male and female fraudsters who work together, this couple has access to hundreds of different bank account details and systematically attempts to perform takeovers of these accounts. They use the phone channel to change the personal details of account holders, such as their address and phone number, while the actual transactions often occur in other channels.

Polite Welsh Lady
This woman with a slight Welsh accent is one of the most effective fraudsters Pindrop® Labs has come across this year. She is extremely friendly, well-spoken, and able to put most call centre agents at ease. Her social engineering skills become even more obvious in cases where she does not hold the correct account information but is able to get the correct information from the agent by successfully controlling the conversation. With these tactics, she has been able to make successful fund transfers of several thousand pounds from a large number of accounts.

The Actress
This is a female fraudster who calls from a service centre on behalf of other people who ‘do not speak English’ very well. Notable in the social engineering space for her voice impersonations, she often switches between the ‘actual customer’ and herself on the same call. She’s able to sound like a male, female, or even a young boy. Despite her somewhat unusual approach to voice impersonation, she is very successful in achieving her goals.

Distorted Please
This fraudster uses voice distortion software to manipulate his voice by lowering or increasing the pitch. The high-pitch voice is used to attack accounts of female account holders. Even with the disguised voice, this fraudster has a very characteristic way of speaking—with the word ‘please’ being his most obvious giveaway. Despite the audibly poor attempt at voice disguise, this fraudster has attacked many accounts and successfully transferred balances.
INDUSTRY VIEW

Fraud rates can vary widely across industries and are dependent upon many factors, including the sophistication of defenses and the size of an organisation. One thing that remains the same is that criminals go where they can find the money.

Banks and Brokerages

In 2016, the fraud rate for global banks was 1 in 867 calls, a 61% increase over 2015’s one in 1,400 calls and higher than the fraud rate across all industries. The trend toward higher fraud rates in financial institutions isn’t unique to banks. For brokerages, 2016 saw a 53% increase in the call centre fraud rate, with 1 in 1761 calls being fraudulent.

Card Issuers

Fraudsters continue to hit card issuers hard. Nearly 1 in 800 calls to a card issuer’s call centre is fraudulent. Criminals of all kinds value stolen credit card numbers because they’re the easiest and fastest way to steal large amounts of money with the lowest chance of detection. Fraud exposure for card issuers is also very high at an average of £267 million in 2016, pointing to the fact that fraudsters increasingly target high-value accounts.

Insurance

The insurance industry is also taking a severe hit from phone fraud. In 2016, one in every 4,700 calls was fraudulent compared to 1 in 12,000 in 2015. Phone fraud groups run a variety of scams against insurance companies, and victims may not notice for a long time, if ever. Most customers rarely call their insurance companies, so fraudsters can have access to a compromised account for months or years. Life insurance policies typically have high cash values and fraudsters are known to take out loans against a victim’s policy or even cash out the policy altogether.

Device Insurance

By far, the highest fraud rate of any single industry is seen in the device insurance sector. For companies that provide payments to consumers whose mobile phones are lost or stolen, 1 in every 194 calls is fraudulent. That rate increased 55% over 2015, when device insurance already had the highest phone fraud rate of any vertical.

GLOBAL FINANCIAL INSTITUTION FRAUD RATES

<table>
<thead>
<tr>
<th>Industry</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Issuer</td>
<td>1 in 900</td>
<td>1 in 800</td>
<td>1 in 867</td>
</tr>
<tr>
<td>Bank</td>
<td>1 in 2650</td>
<td>1 in 1400</td>
<td>1 in 1761</td>
</tr>
<tr>
<td>Brokerage</td>
<td>1 in 3000</td>
<td>1 in 2700</td>
<td></td>
</tr>
</tbody>
</table>

GLOBAL INDUSTRY FRAUD RATES

<table>
<thead>
<tr>
<th>Industry</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insurance</td>
<td>1 in 12000</td>
<td>1 in 4700</td>
</tr>
<tr>
<td>Retail</td>
<td>1 in 1000</td>
<td>1 in 491</td>
</tr>
</tbody>
</table>

Fraud rate is calculated as fraudulent calls per legitimate calls
Retail

Fraud rings have also taken aim at retail call centres in 2016, as the confluence of contactless payment rollouts and better online security has pushed fraudsters to exploit the phone channel. In 2014, one in 1000 calls to a retail call centre was fraudulent. In 2016, that number jumped to 1 in 491. For retailers, this trend will be difficult to reverse without a major change in the way they handle call centre security.

Fraudsters continue to perfect their tactics and the huge volume of stolen information available from data breaches means they have access to better and more accurate data about potential victims. Some of the scams hitting retail chains are fiendishly clever and quite difficult to stop. For example, rather than stealing a victim’s payment card data, some scammers specifically target a consumer’s loyalty account. In much the same way that they perform account takeovers at banks, scammers will make multiple calls to retail loyalty account call centres to try and reset account passwords or change other account details. The loyalty points generated by shopping at some retail chains are as good as cash, so fraudsters will gain access to those accounts and then use them to purchase goods. In some cases, they will even buy new items and send them to the victim just to get the loyalty points a new purchase accrues. Similar scams have been seen in hotel and airline loyalty programs.

METHODOLOGY

For this report, Pindrop® Labs analysed millions of calls globally using Phoneprinting™ technology to dissect the details of attacker techniques and behaviour. Pindrop’s patented Phoneprinting™ technology was combined with metadata and voice biometrics analysis of the phone call audio content. Phoneprinting™ technology measures 147 characteristics of the audio signal in order to form a unique fingerprint for the call. This information provides an unprecedented level of insight into the phone channel. Phoneprinting™ technology determines a caller’s true location and device type. In addition, it helps to identify multiple callers associated with the same phoneprint, allowing enterprises to track fraud rings.