intelligent authentication conference

26-27 April 2016 LONDON, ENGLAND

Phone Fraud Battlefield

Morris Pentel

CXFO.org

pindrop

Telephone fraud is up by 92%.

Is this a real threat or just some marketing hype

Has Fraud changed?

Is Contact Centre an easy target?

Is Contact Centre a more valuable target?

Why is it important ?

Are we are just finding more?

CXFO.org

pindrop

Is it now an arms race?

Financial Fraud Action UK
Working together to prevent fraud

It was recently announced that Phone Fraud is up by 92% this year. Research by the Financial Fraud Action UK (FFA UK) found that five million frauds occur every year across England and Wales, costing the UK around £24bn.

June 2015 - Overall, more than 86.2 million calls per month in the U.S. are phone scams
Pindrop

CXFO.org

pindrop

Has Fraud changed?

Industrialisation of Fraud - Its now really Big Business

Focus of industrial scale investment by Fraudsters to exploit opportunities for fast returns

Increased attacks on *consumers* & *contact centre* focused on gaining information to create the financial crime

KPMG

KPMG's UK Fraud Barometer saw a marked increase in fraudsters targeting individuals and families, particularly those in financial distress, stealing £156m.

This reflects a 300% increase on 2014 when just £38.5m was lost by vulnerable victims.

CXFO.org

pindrop

What has changed are the size and scale of the operations?

SECURITY today

Rise in Social Engineering Fraud

Attackers using social engineering have found the phone channel to be the weakest link for corporations and consumers.

This trend will continue in 2016 as fraud schemes become more and more creative. Hackers impersonating customer support people, IRS agents, and even security specialists claiming to have detected fraud will continue to be a source of stealing personal financial data.

CXFO.org

pindrop

What has changed are the size and scale of the operations?

SECURITY today

Rise in Social Engineering Fraud

Attackers using social engineering have found the phone channel to be the weakest link for corporations and consumers.

This trend will continue in 2016 as fraud schemes become more and more creative. Hackers impersonating customer support people, IRS agents, and even security specialists claiming to have detected fraud will continue to be a source of stealing personal financial data.

the guardian

As security systems have improved in other areas of banking, fraudsters have opted to target consumers directly by phoning them up, or using online vulnerabilities.

Scammers have pretended to be bank staff, police and from firms such as TalkTalk, and persuaded consumers to send money to their bank accounts, aided by the faster payments system and previously lax account opening requirements at banks.

CXFO.org

pindrop

What has changed are the size and scale of the operations?

SECURITY today

Rise in Social Engineering Fraud

Attackers using social engineering have found the phone channel to be the weakest link for corporations and consumers.

This trend will continue in 2016 as fraud schemes become more and more creative. Hackers impersonating customer support people, IRS agents, and even security specialists claiming to have detected fraud will continue to be a source of stealing personal financial data.

the guardian

As security systems have improved in other areas of banking, fraudsters have opted to target consumers directly by phoning them up, or using online vulnerabilities.

Scammers have pretended to be bank staff, police and from firms such as TalkTalk, and persuaded consumers to send money to their bank accounts, aided by the faster payments system and previously lax account opening requirements at banks.

Mail Online

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | Video | Tr

Latest Headlines | News | World News | Arts | Headlines | Pictures | Most read | News Board | Wires

Bank customers warned over new 'number spoofing' con: 95% rise in telephone banking thefts as fraudsters are impersonating firms on caller ID to steal millions from accounts

- Scammers copy numbers of banks and the police to gain trust from victims
- They also send texts which appear as a genuine message from the bank
- Fraudsters then convince customers to hand over their PIN and passwords
- Some even persuade victims to transfer money directly into their account
- One pensioner was tricked by number spoofers into handing over £12,000

By SIMON TOMLINSON FOR MAILONLINE

DON'T

TOWIE's Wright ar battle it o swimwea on a yach Plenty of curves on

'I've no

CXFO.org

pindrop

What has changed are the size and scale of the operations?

SECURITY today

Rise in Social Engineering Fraud

Attackers using social engineering have found the phone channel to be the weakest link for corporations and consumers.

This trend will continue in 2016 as fraud schemes become more and more creative. Hackers impersonating customer support people, IRS agents, and even security specialists claiming to have detected fraud will continue to be a source of stealing personal financial data.

the guardian

As security systems have improved in other areas of banking, fraudsters have opted to target consumers directly by phoning them up, or using online vulnerabilities.

Scammers have pretended to be bank staff, police and from firms such as TalkTalk, and persuaded consumers to send money to their bank accounts, aided by the faster payments system and previously lax account opening requirements at banks.


Mail Online

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | Video

Latest Headlines | News | World News | Arts | Headlines | Pictures | Most read | News Board | Wires

Bank customers warned over new 'number spoofing' con: 95% rise in telephone banking thefts as fraudsters are impersonating firms on caller ID to steal millions from accounts

- Scammers copy numbers of banks and the police to gain trust from victims
- They also send texts which appear as a genuine message from the bank
- Fraudsters then convince customers to hand over their PIN and passwords
- Some even persuade victims to transfer money directly into their account
- One pensioner was tricked by number spoofers into handing over £12,000

By SIMON TOMLINSON FOR MAIL ONLINE

Gang Fraud


THE WALL STREET JOURNAL.

Subscribe Now | Sign In

SPECIAL OFFER: JOIN NOW

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

ELECTION 2016 Populist Campaign Tone Rankles ... | Ted Cruz and John Kasich Team Up to Stop Donald Trump | Trump, Clinton Hold Big Leads in Pennsylvania | U.S. Military Role in Syria Expanding

YOU ARE READING A PREVIEW OF A PAID ARTICLE. SUBSCRIBE NOW TO GET MORE GREAT CONTENT.

U.S.

More Street Gangs Turn to Financial Crimes

Check fraud and identity theft can be lucrative and hard to detect, experts say

Legal Practice Management Software APPF

"The sums of money involved are staggering - Even though it's a small minority...the potential amount of money involved and damage to people's financial accounts is greatly out of proportion to other gang crimes."

Ron Huff, a criminology professor at the University of California, Irvine, who studies gangs.

CXFO.org

pindrop

Overall

Gang Fraud

"The sums of money involved are staggering," said Ron Huff, a criminology professor at the University of California, Irvine, who studies gangs.

"Even though it's a small minority...the potential amount of money involved and damage to people's financial accounts is greatly out of proportion to other gang crimes."

KPMG's UK Fraud Barometer saw a marked increase in fraudsters targeting individuals and families, particularly those in financial distress, stealing £156m.

This reflects a 300% increase on 2014 when just £38.5m was lost by vulnerable victims.

Financial Fraud Action UK
Working together to prevent fraud

Mail Online

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | Video

Latest Headlines | News | World News | Arts | Headlines | Pictures | Most read | News Board | Wires

Bank customers warned over new 'number spoofing' con: 95% rise in telephone banking thefts as fraudsters are impersonating firms on caller ID to steal millions from accounts

- Scammers copy numbers of banks and the police to gain trust from victims
- They also send texts which appear as a genuine message from the bank
- Fraudsters then convince customers to hand over their PIN and passwords
- Some even persuade victims to transfer money directly into their account
- One pensioner was tricked by number spoofers into handing over £12,000

By SIMON TOMLINSON FOR MAILONLINE

$35,000 a minute - USA

Consumers that don't trust their financial institutions (don't use the services offered by them) suffer more damage if they become fraud victims.

Consumers that do not trust their financial institutions are less likely to use transaction monitoring, email alerts, credit freezes and black market monitoring

-their information being used for 75 percent longer by fraudsters

- incurring a 185 percent greater mean consumer expense than those victims that have high trust in their financial institutions

Source Javelin

Fraud = $35,000 a minute - USA

JAVELIN

ercrime

UK businesses battling huge rise in cybercrime, report says

PwC says not enough companies are dealing with big threat of economic crime and problem of 'silver fraudsters'

Davies

Save for Later

Ashley Madison, the adultery website, suffered a very high-profile security breach in 2015. Photograph: Lauren Hartley/PA

UK businesses are battling a huge rise in cybercrime capable of bringing down entire companies, according to analysis by accountancy company PwC.

In a report that singled out the UK as a hotbed of economic crime, PwC said the threat of cyber offences was now a "board-level issue", but warned that not enough companies were taking it seriously enough.

PwC also warned of a surge in the number of "silver fraudsters" - older staff who turn against their employer.

Approximately 55% of UK firms have fallen victim to economic crime in the past two years, according to the PwC global economic crime surveys, compared with a

Definite Increases – across majority of studies across majority of Fraud types across the world

Rise in Social Engineering Fraud

SECURITY today

Attackers using social engineering have found the phone channel to be the weakest link for corporations and consumers.

This trend will continue in 2016 as fraud schemes become more and more creative. Hackers impersonating customer support people, IRS agents, and even security specialists claiming to have detected fraud will continue to be a source of stealing personal financial data.

the guardian

As security systems have improved in other areas of banking, fraudsters have opted to target consumers directly by phoning them up, or using online vulnerabilities.

Scammers have pretended to be bank staff, police and from firms such as TalkTalk, and persuaded consumers to send money to their bank accounts, aided by the faster payments system and previously lax account opening requirements at banks.

CXFO.org

pindrop

What has changed are the size and scale of the operations?

"We know that it is a worsening problem as this year we have seen a dramatic increase in the number of reports about dodgy calls.

I think that they have found us to be vulnerable and now it's like, there is a gang of them hanging around outside the virtual borders of our operation and our staff are developing a siege mentality. Its difficult because they are not stealing from us in the traditional sense but it is still making life more and more uncomfortable."

Contact Centre Director - Major Utility

CXFO.org

pindrop

New Focuses

Increased attacks on *consumers* & *contact centre* focused on gaining information to create the financial crime

Increase in secondary attacks

Increase in value of data for attacks on KBA (knowledge-based authentication) protected funds

As consumers have gone Omni-Channel so has Fraud

The inbound telephone channel is now becoming a focal point of attack for fraudsters

CXFO.org

pindrop

New Tricks and Old ones

Increasing evidence of sophistication in technology

Masked phone calls routed through complex technology and international services

Masked voices through clever technology or cheap apps or old fashioned acting

Available in the app store

CXFO.org

pindrop

Strategic advantage - Bad Guys

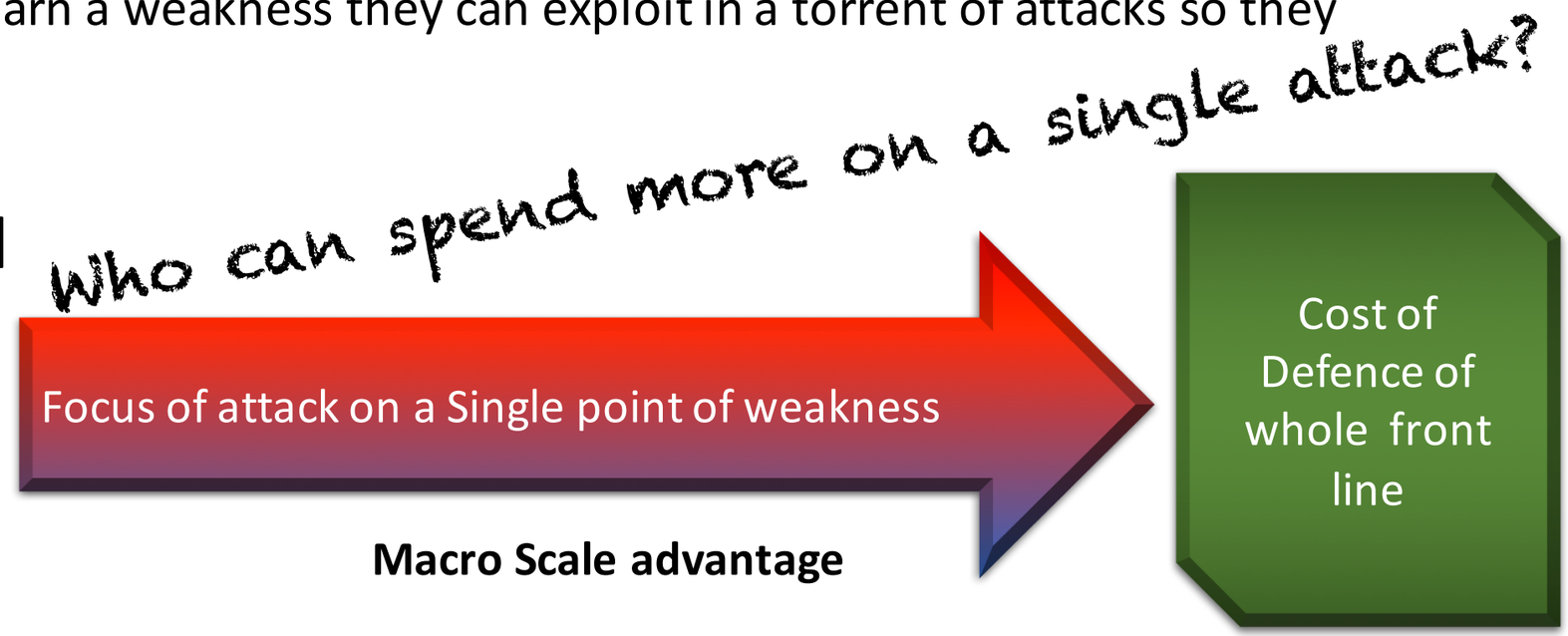
The agent is an obvious target

Fraudsters get more practice than agents – its their job

Agent listens carefully but it may be only one in a hundred or a thousand calls for that one agent while the fraudster may learn a weakness they can exploit in a torrent of attacks so they can get is information.

Fraudsters hide in a crowd

Better informed



CXFO.org

pindrop

Strategic advantage - Bad Guys

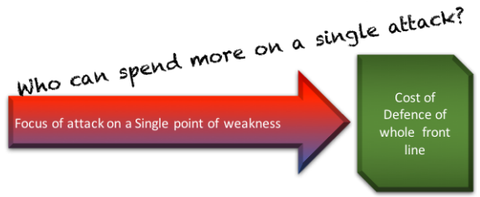
Fraudsters get more practice than agents – its their job

Agent listens carefully but it may be only one in a hundred or a thousand calls for that one agent while the fraudster may learn a weakness they can exploit in a torrent of attacks so they can get is information.

Fraudsters hide in a crowd

Better informed

Macro Scale advantage



Every successful attack fuels the appetite for more and funds the next attack

Organisations failed to act quickly enough about Cyber Crime and *now are funding both sides of the war*

Will we make the mistake of not investing quickly enough fuelling the pace of growth of KBA Intrusion

KBA Intrusion has a lower priority than actual financial attack and is not as noticeable and has less direct impact in the transactional sence

CXFO.org

pindrop

Improvements in Detection

Innovations in many connected fields are joining together

Phoneprinting technology tests on the existing phone calls & data sometimes - 3 or 5 times the size of the problem they thought they had

Behavioral science analytics technology detecting patterns of Fraud improving

Other technologies such as Biometrics EMV etc. are all closing loopholes

We are finding more of what has been going on

CXFO.org

pindrop

Is it now an arms race?

Improvements in detection on other channels may make them less attractive and *increase the appetite for phone attacks*

If CC Owners fail to act quickly it will be perceived as an easy target creating an incentive for phone fraud

Long Term Impact of failure to invest

More Battles with Fraudsters requiring More Investment over a long timescale – Everyone will have to invest but who ever invests more first leads the arms race and also if the white hats move quickly they may stifle the incentive to invest by criminals

CXFO.org

pindrop

What is the CX Risk?

The agent is an obvious target

Constantly balancing between being helpful to deliver a great customer experience and following protocol and best practice agent behaviour can become predictable

Was it your agent that gave the last piece of information needed to commit a fraud?

How about angry Customers?

CXFO.org

pindrop

Customers viewpoint

Phone Attacks will have much more significant impacts on Customer Experience than Cyber Fraud because *it happens to the Customer*

It also impacts how you treat your customer on the phone – their phone experience

KBA costs increase and must become less effective

Increased Fraud would mean increased overt security

CXFO.org

pindrop

Consumers that don't trust their financial institutions (don't use the services offered by them) suffer more damage if they become fraud victims.

Consumers that do not trust their financial institutions are less likely to use transaction monitoring, email alerts, credit freezes and black market monitoring

-their information being used for 75 percent longer by fraudsters

- incurring a 185 percent greater mean consumer expense than those victims that have high trust in their financial institutions

Source Javelin

Fraud = $35,000 a minute - USA

CXFO.org

pindrop

Customers

Customers are already better at doing business with you, than you are at doing business with them!

You are competing to be the source of info

More sources of information
More up to date
More in-depth Information about your proposition
More information about you than your front line
Effective Language

CXFO.org

pindrop

Customers are already better at doing business with you, than you are at doing business with them!

Customers

For the first time in history, consumers now have much better technology than the enterprises that serve them

Where enterprises are spending **billions** consumers are spending tens of **trillions** and the gap is growing
The pace of change is creating a larger and larger gap in capability

BYOD & BYOE*(xperience)*

CXFO.org

pindrop

Customers are already better at doing business with you, than you are at doing business with them!

Customers

Choice of Technology (end point device such as phone or tablet) is no longer a barrier to experience or functionality

Choice of Supplier – Amazon UK has 100 ml products and fastest growing banks and Telcos' are the Supermarkets

CXFO.org

pindrop

Customers

Customers are already better at doing business with you, than you are at doing business with them!

How many channels do you use as work?

As Digital Customers we use more than 6/7 but organisations we struggle with 3

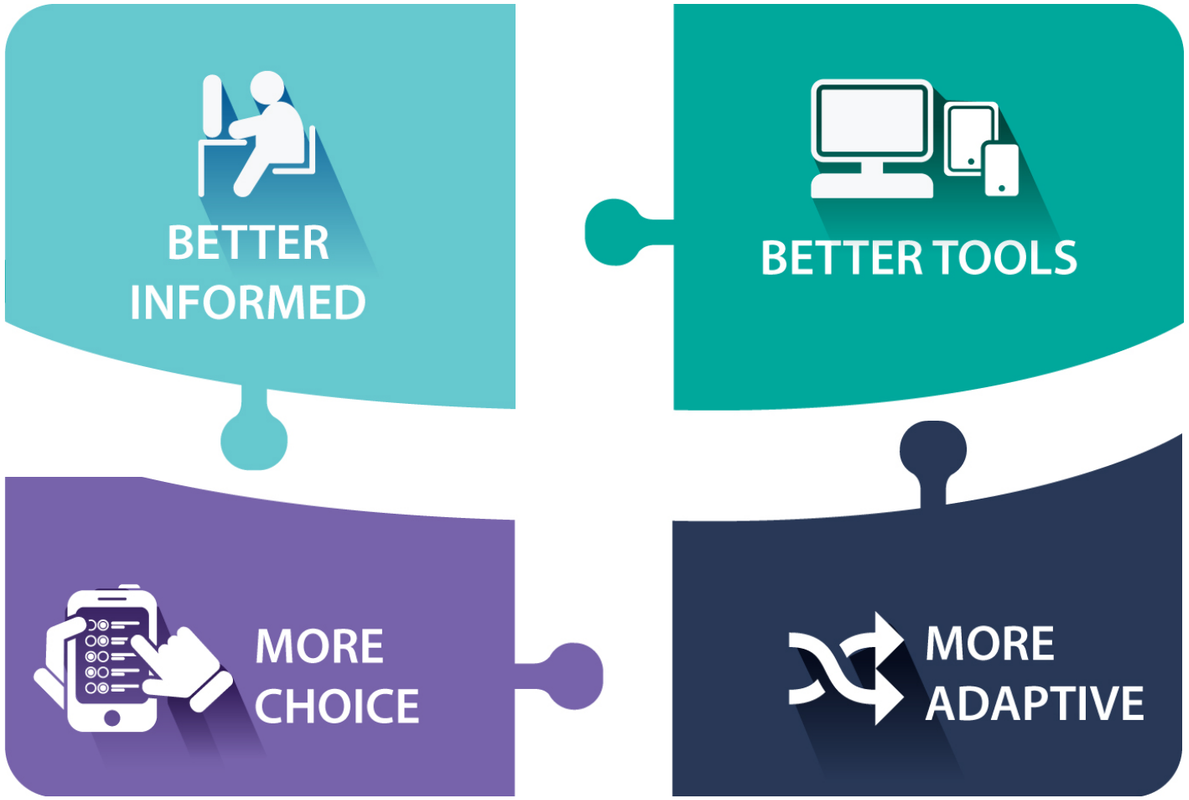
The pace of Customer adoption is **18 months** which is ***less than half*** of organisational adoption

CXFO.org

pindrop

If customers are already better at doing business with you what about…

Fraudsters



CXFO.org

pindrop


WHAT IF YOUR FAVOURITE PUB
WAS RUN LIKE YOUR BANK?

What happens if we don’t act?

Will we start to experience airport like inconvenience for our protection?

Think about the impact on Customer Experience and the impact on your day to day relationship with your customer

What is the solution?

- Reliance on KBA alone is no longer an option
- A continuous programme of action across all channels to create an Omni-Channel approach
- A blended process & technology strategy across all activities – thinking about Fraud as a series of experiences rather than a single smash & grab raid

CXFO.org

pindrop

And finally

There is an increase in Fraud overall and a dramatic increase in phone Fraud

Our Customer Relationships are at risk of phone Fraud because it is a human experience

We are not yet treating intrusions with the same seriousness as attempted theft

We are getting better at detecting it because of new technologies

We need to create a shield of all types of technologies across all our channels or *weak* points will become *focal* points

CXFO.org

pindrop

Customer Experience Foundation

Google Me

Morris Pentel

Google Search I'm Feeling Lucky

@MorrisPentel

m@pentel.me

Find me on

CXFO.org

E-books (2)
White Papers (20+)
Customer Events
Films (5) Radio (2)
Articles 100+ (6 Languages)
Workshops 20+ per Annum
Conferences 20+ per Annum

Thank You

CXFO.org

pindrop