# COMMERCIAL BANKING FRAUD


UK businesses impacted

Increase in Digital fraud

COMMERCIAL BANKING

# COMMERCIAL BANKING – FRAUD AWARENESS & GUIDANCE

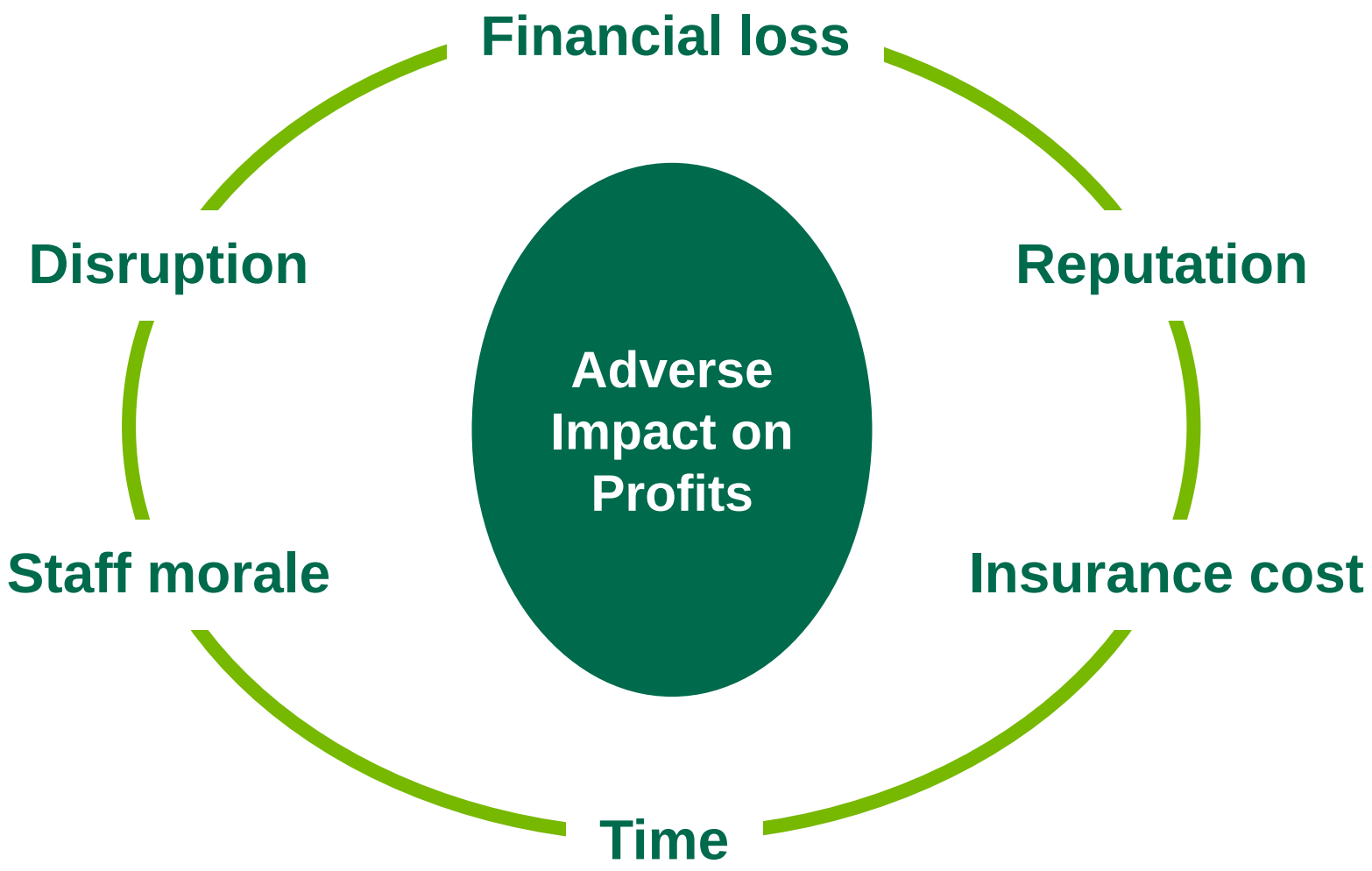
Chris Fawcett,
Commercial Fraud Manager

North Mid Markets, Newcastle
March 2016

# AGENDA

- Impacts
- Common Areas of Vulnerability
- Social Engineering - Underpin
- Vishing – Telephone Scam
- Malware
- Mandate Fraud
- Impersonation Fraud/Email Hacking
- Advice & Guidance

# POTENTIAL OUTCOMES



# THERE ARE SOME COMMON FACTORS THAT INCREASE VULNERABILITY

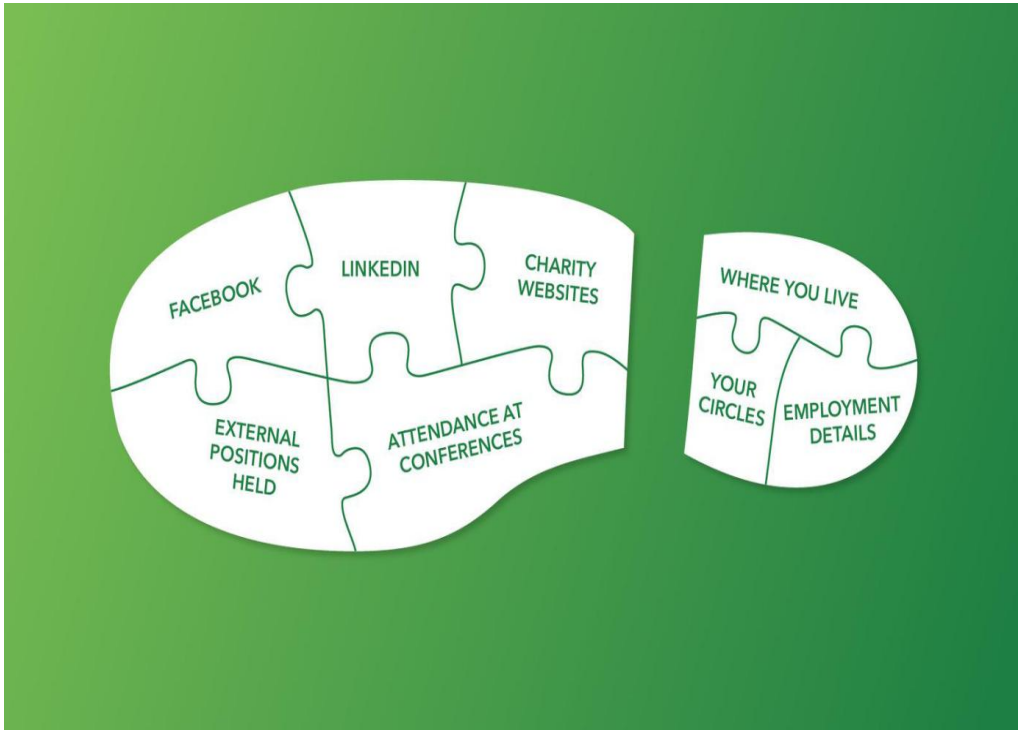
- Low threat awareness
- Poor cyber hygiene
- Complacent, untrained, unaware payments teams
- Inadequate controls, procedures and processes
- Victims react after a fraud has taken place

# SOME OF THE POSSIBLE REASONS WHY THIS ENVIRONMENT EXISTS

- Cost fraud is difficult to measure (5.47% of expenditure)
- Prudent approach to factor in
- Almost all other costs are managed
- Denial that the threat is real. Probably won't happen!
- Not seen as a priority

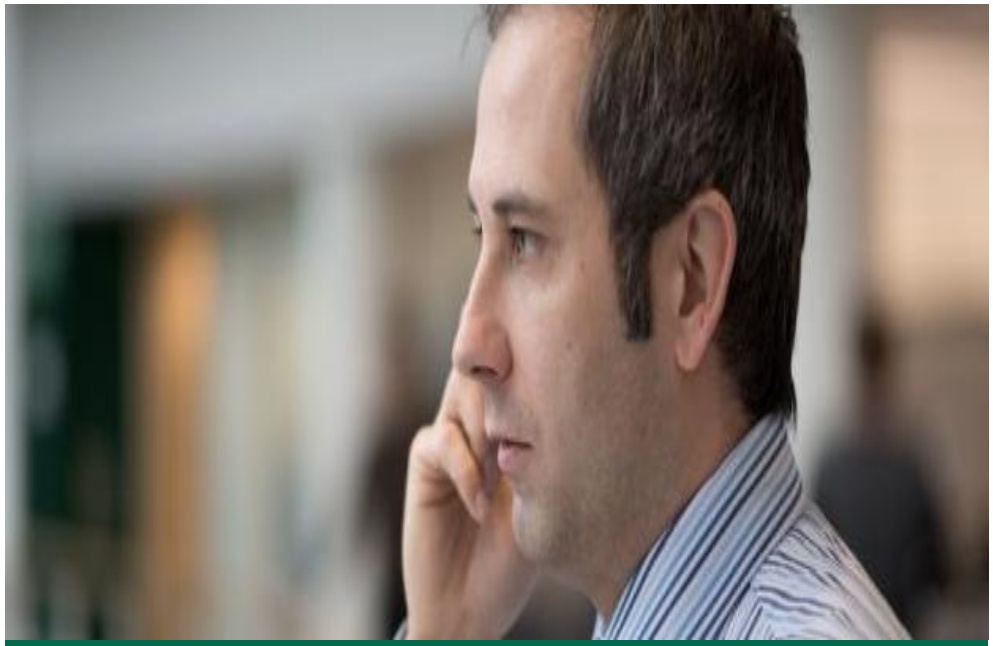
# THE ORGANISED FRAUDSTER HAS TIME TO RESEARCH KEY INFORMATION BEFORE THE ATTACK

- Social Engineering used to obtain confidential information
- Prior phone calls
- Social media researching key officials
- Trading partners/supplier/ contractor information
- Financial information



# WE HAVE SEEN A SIGNIFICANT INCREASE OF CUSTOMERS ATTACKED BY VISHING

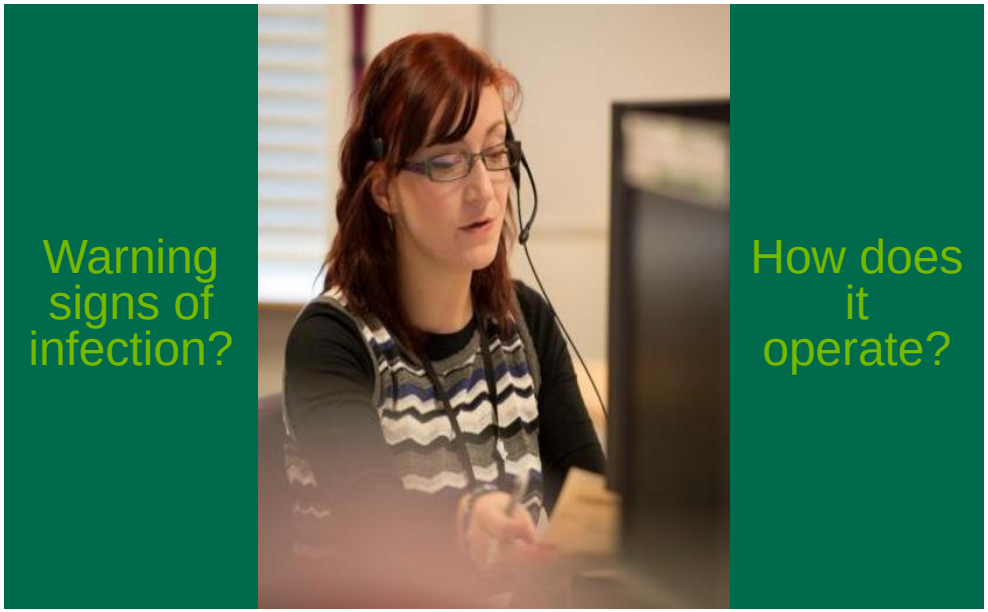
- Their objectives
- Savvy calls
- Techniques used
- Finding the money
- Client liability



Social Engineering - Telephone Scam

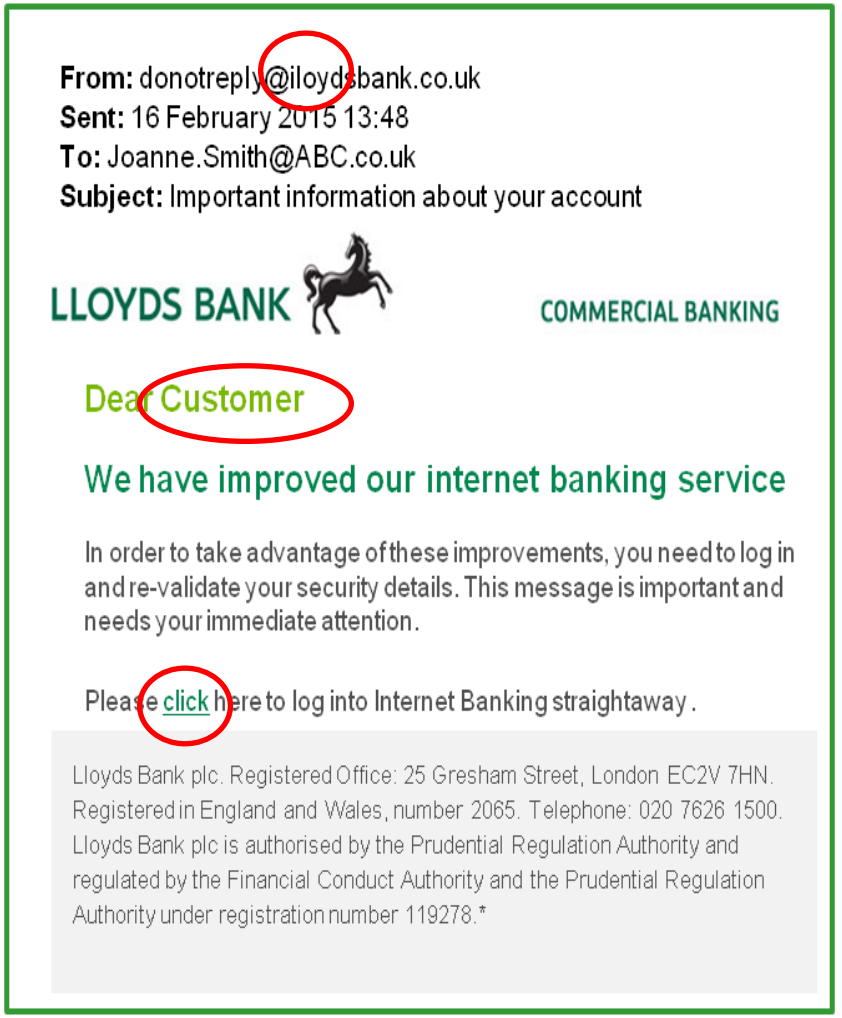
# MALWARE IS A KEY DRIVER BEHIND THE 40% HIKE IN DIGITAL FRAUD

- Spear phishing campaigns/Malvertising
- Potential warning signs
- Malware operates in different ways
- Strains evolve and mutate
- Ransomware – data encryption



# THERE ARE SOME PRACTICAL STEPS THAT YOU CAN IMPLEMENT TO PROTECT YOUR BUSINESS

- Authenticate calls
- Install high quality Security Software – regular updates. No guarantee!
- Think before you click!
- Be aware, never disclose!
- Strong passwords and online banking security settings
- Back up critical data regularly



**From:** donotreply@iloydsbank.co.uk
**Sent:** 16 February 2015 13:48
**To:** Joanne.Smith@ABC.co.uk
**Subject:** Important information about your account

LLOYDS BANK COMMERCIAL BANKING

Dear Customer

We have improved our internet banking service

In order to take advantage of these improvements, you need to log in and re-validate your security details. This message is important and needs your immediate attention.

Please click here to log into Internet Banking straightaway.

Lloyds Bank plc. Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales, number 2065. Telephone: 020 7626 1500. Lloyds Bank plc is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under registration number 119278.*

# FRAUD PREVENTION – LAYERED APPROACH IS STRONGLY RECOMMENDED

# OUR DIGITAL PRIORITIES

LLOYDS BANKING GROUP

**>£1bn**

DIGITAL INVESTMENT BETWEEN 2015 – 2018

# MANDATE/INVOICE SCAMS ARE VERY ACTIVE FRAUDS TARGETING ALL COMMERCIAL SECTORS

- Instruction to change account details
- Research and phone call to add legitimacy
- Build trust/relationship with the Finance team
- Redirection of all future payments
- Time to move the money. Slim chance of recovery

# EMAIL HACKING & SPOOFING (CEO FRAUD) HAS BEEN A RAPIDLY ESCALATING FRAUD DURING 2015

LLOYDS BANKING GROUP

- Impersonation by hacking into or spoofing a senior executive's email account
- Instruction to Finance or Payments team
- Urgent payment to specified account
- Familiar terminology
- Fear to challenge the instruction or unable to contact the sender

# STAFF AWARENESS IS A VITAL CONTROL IN PREVENTING A BUSINESS FALLING VICTIM

- Be cautious, remain vigilant
- Authenticate the instruction
- Raise client awareness
- Documented procedure
- Report to Bank and Action Fraud

# THERE ARE 5 KEY FRAUD PREVENTION TIPS THAT WE RECOMMEND ALL BUSINESS LEADERS IMPLEMENT

- Be proactive
- Establish hiring procedures
- Train employees in fraud prevention
- Implement a fraud hotline
- Set the tone

# THERE IS SOME EXCELLENT INFORMATION AVAILABLE THAT YOU CAN USE TO HELP EDUCATE YOUR STAFF

- Bank Relationship Manager
- Lloyds/Bank of Scotland Client Fraud Awareness brochure
- Visit websites
- Webcast recordings
- Other websites
  - Get Safe Online
  - Action Fraud
  - City of London/Met Police

# QUESTIONS?

# SUMMARY

- Impacts
- Common Areas of Vulnerability
- Social Engineering
- Vishing – Telephone scam
- Malware
- Invoice/Mandate Fraud
- Impersonation Fraud - Email Hacking/Spoofing
- Advice & Guidance