Annual Academies Update 2017

Friday 14th July 2017

Newark and Nottinghamshire Showground, Newark

Agenda

- **Managing People Cost Effectively**

  Beststart Human Resources & Irwin Mitchell Solicitors
- **Fraud Guidance**

  Lloyds Bank
- **Break**
- **The Academies Accounts Direction for 2017 and Looking to the Year Ahead From A Financial Perspective**

  Streets Chartered Accountants

Managing People Costs Effectively

Jenny Arrowsmith, Senior Associate Irwin Mitchell LLP

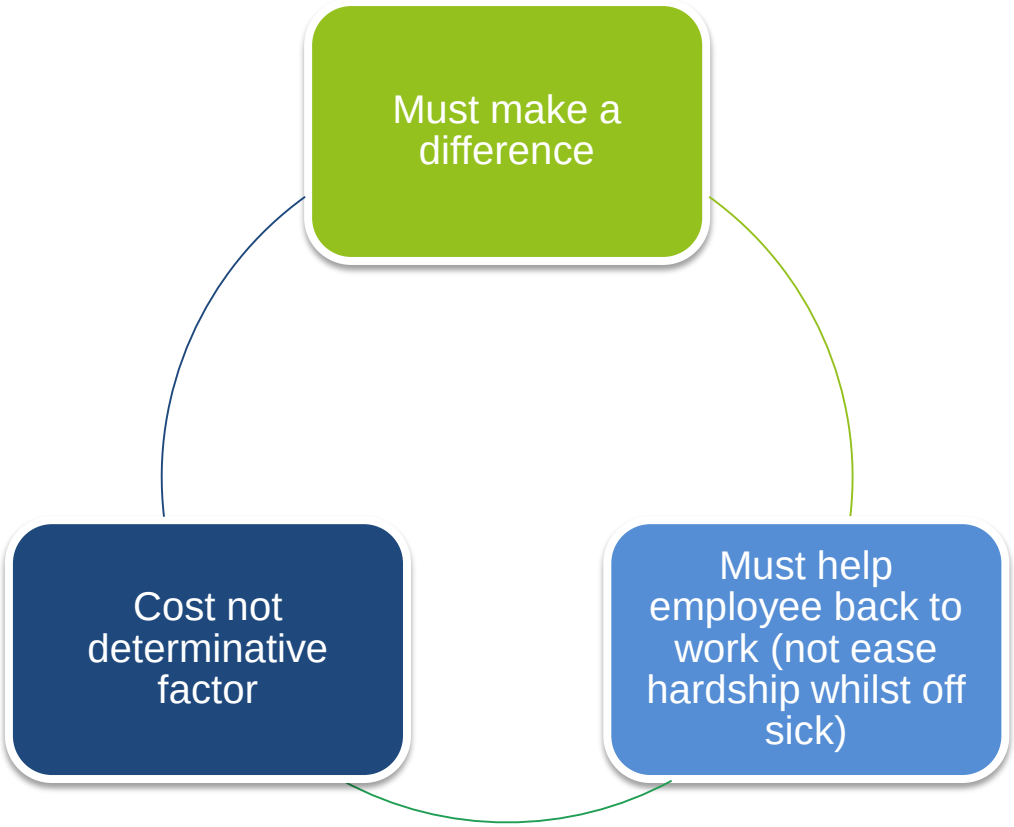
Andrew Hall, HR Consultant Beststart Human Resources

Common themes – to help withstand financial pressures

Reduce your sick pay costs

- Managing short term absence – nil cost but time and effort
- Managing long term absence – significant cost
- You can manage disability related issues
- You can dismiss even before sick pay is exhausted
- Know how to be a “savvy” customer to Occupational Health
- Reasonable Adjustments – know the extent of your obligations
- Seek Legal Advice

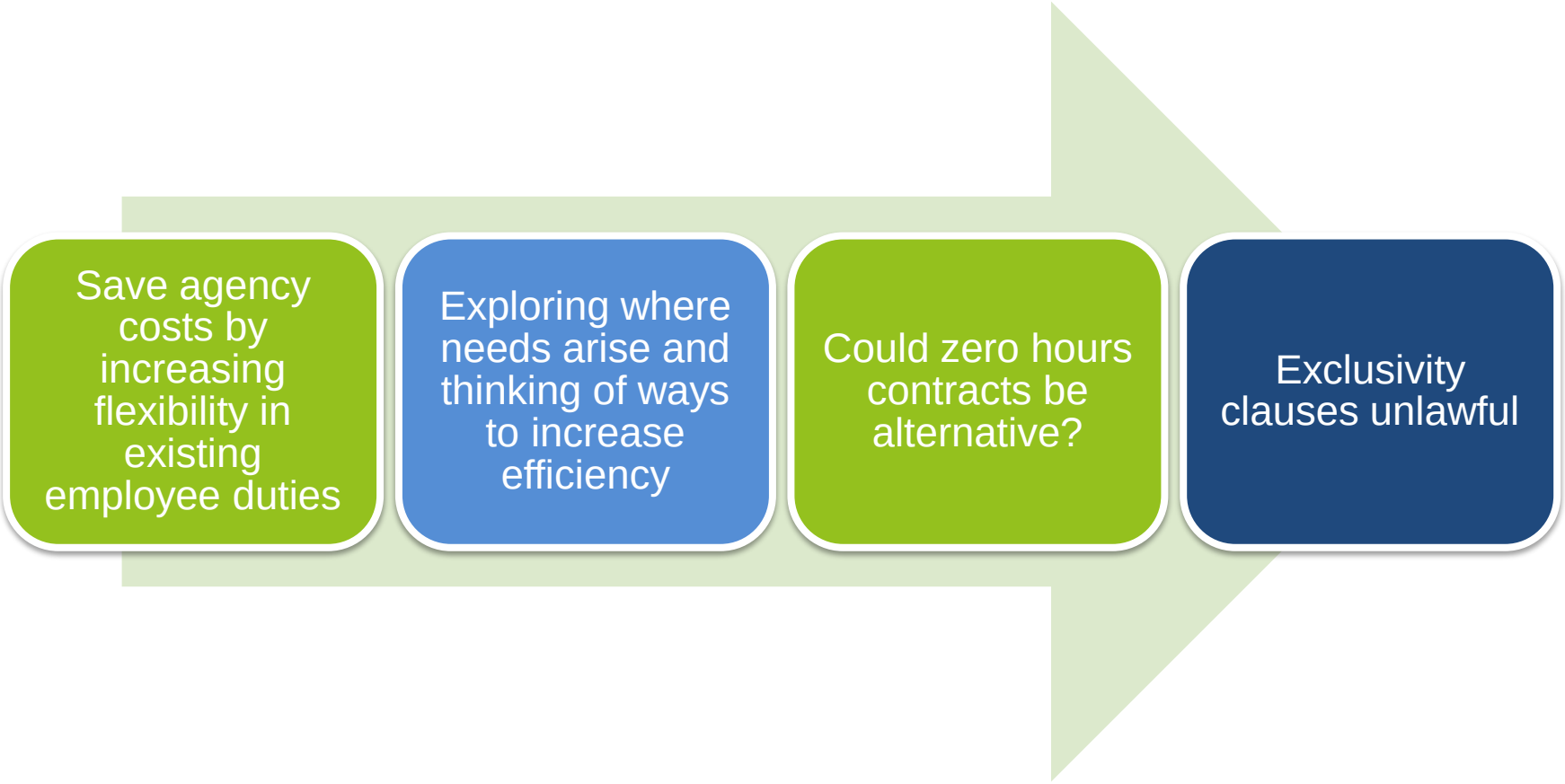
Reasonable adjustments



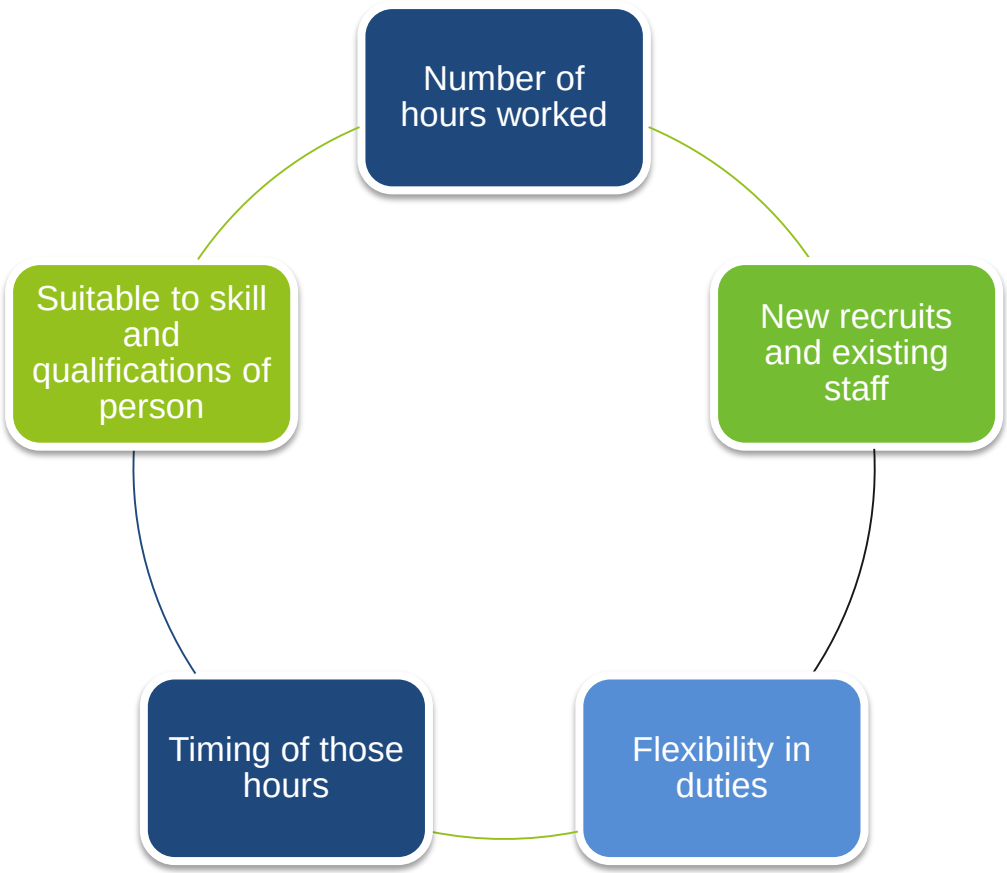
Practical points and tips

- Have a clear policy and process for managing sickness pro-actively. Set expectation.
- Keep in contact; updates, prognosis, correspondence, home visits. Be hands-on where appropriate.
- Seek professional medical advice early on.
- Don’t be afraid to challenge poor attendance levels with formal process

Reduce agency spend



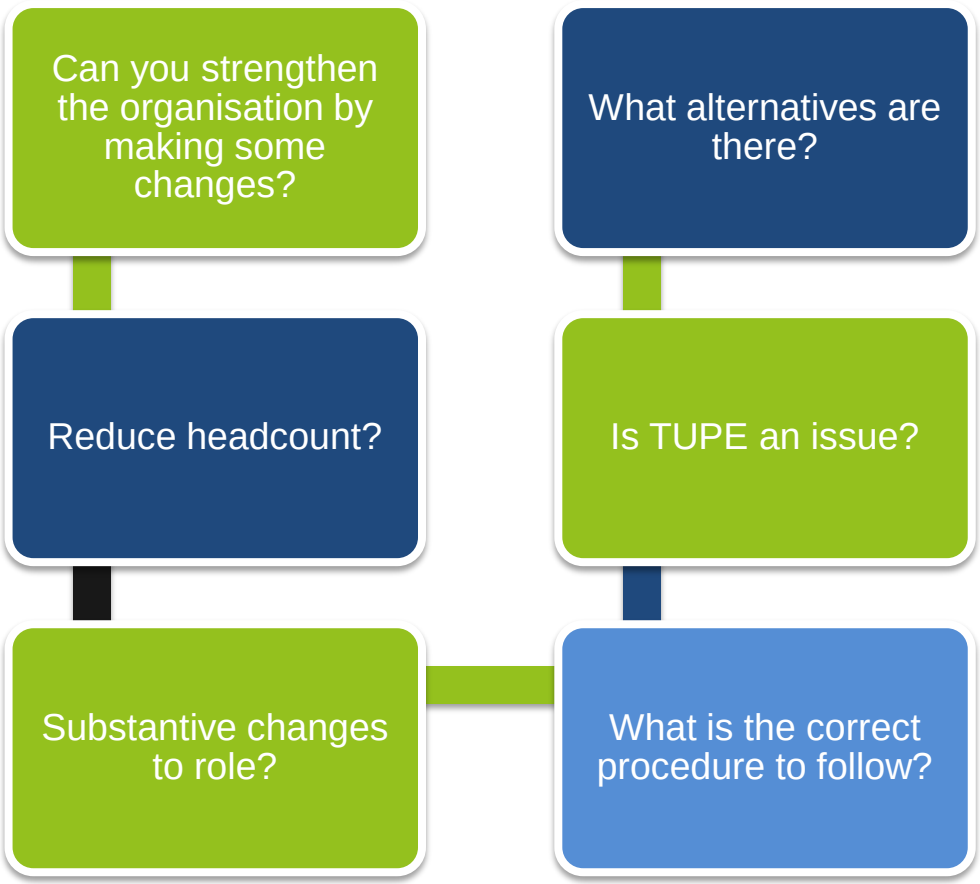
Flexibility in working arrangements



Recruitment/workforce planning

- Review current structures
- Succession planning
- Resignations: an opportunity?
- Is there the same need for the role?

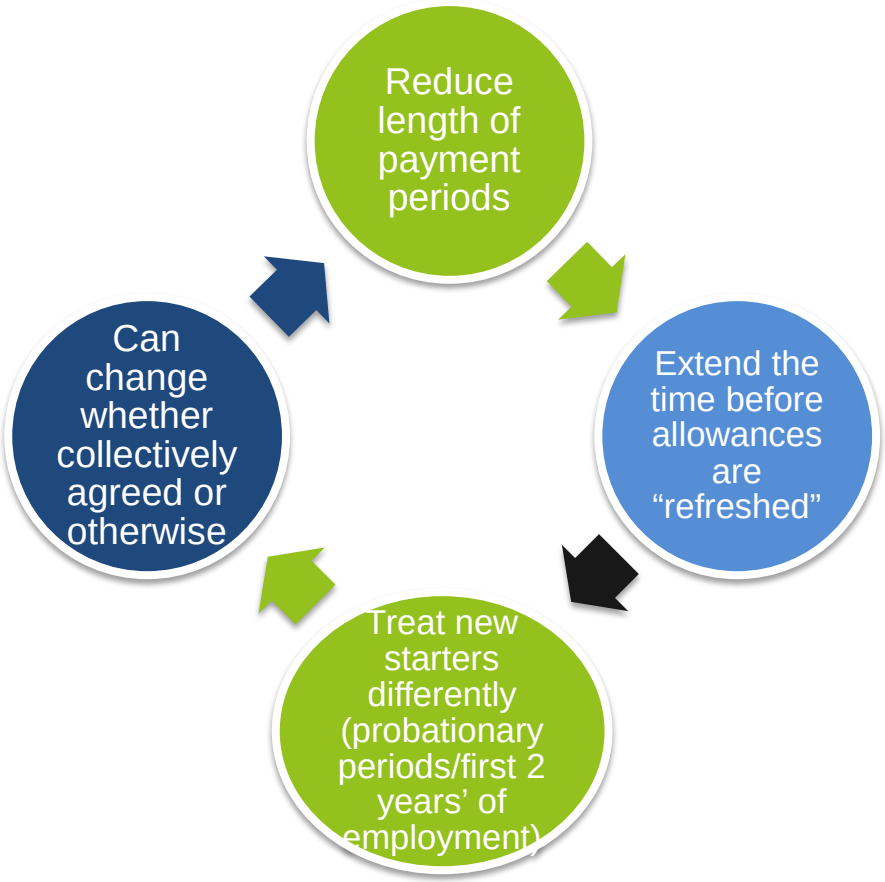
A word about reorganisations



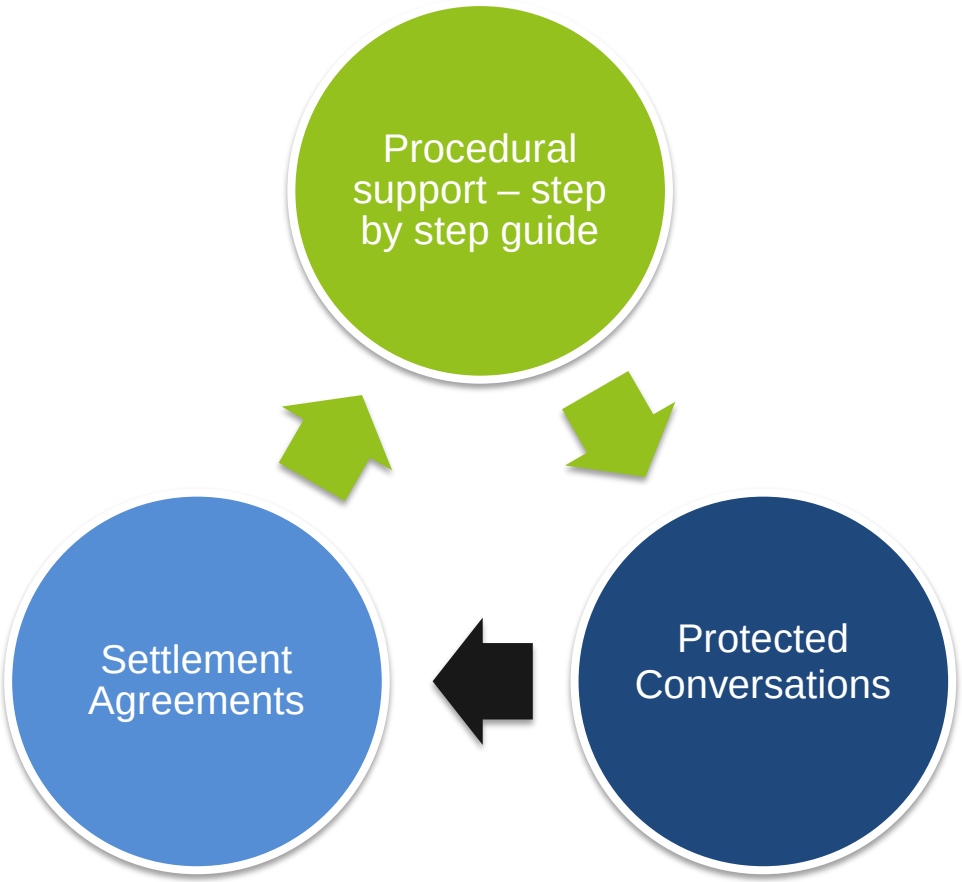
Changing terms and conditions

- Contractual terms vs policies
- Seek agreement to changes
- Dismissal and re-engagement
- Collectively agreed terms
- Changes to strike ballots and mandates
- Effect of TUPE

Changing sick pay arrangements



Legal Tools


Procedural support – step by step guide
Protected Conversations
Settlement Agreements

Key points

1. Don’t accept the status quo
   - Challenge the norm
   - Reform and move with the times

2. Be prepared to look at everything
   - Don’t go for easy option, go for best solution
   - Anything is possible so long as you;

3. Do it right!
   - Seek professional advice and support
   - Manage the process properly

Any questions?

Streets HR

is provided in association with

and

STREETSHR@STREETSWEB.CO.UK

THE GLOBAL CYBER ATTACK OF 2017

150

Countries around the world where the attack has been found

200,000+

Computers affected

*Source: Europol, European Law Enforcement Agency

COMMERCIAL BANKING

Fraud Awareness & Guidance

Helping to protect you and your business

Vin Pandha, Commercial Fraud Manager

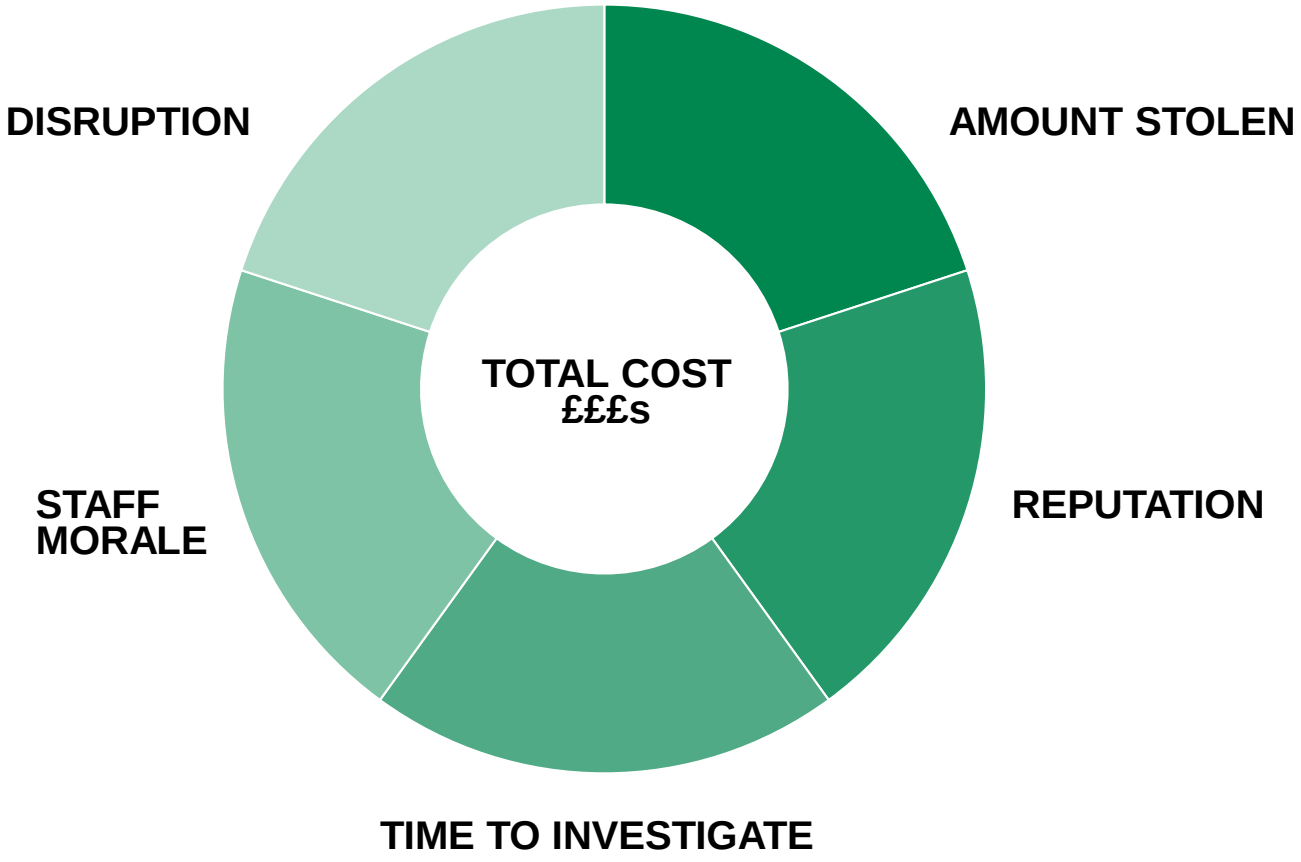
LLOYDS BANKING GROUP

AGENDA

1. Impacts
2. Fraud Attack
   - The Research Phase
   - Launching the Attack
3. Approach to Fraud Risk Management
4. The Fraud Outlook
5. Further Information
6. Questions & Answers

THE TRUE COST OF FRAUD TO VICTIM ORGANISATIONS

Implications can be wide ranging and far reaching.



THE RESEARCH PHASE

Malware, Social Engineering and Social Media

THE MOST PREVALENT BANKING TROJANS OPERATING WORLDWIDE

The agile approach adopted by criminals makes the cyber threat a constant challenge.

- Zeus
- Gozi
- Ramnit
- **Dridex**
- Sphinx
- Client Maximus
- Qadars
- Trickbot
- Gootkit
- Neverquest
- GozNym

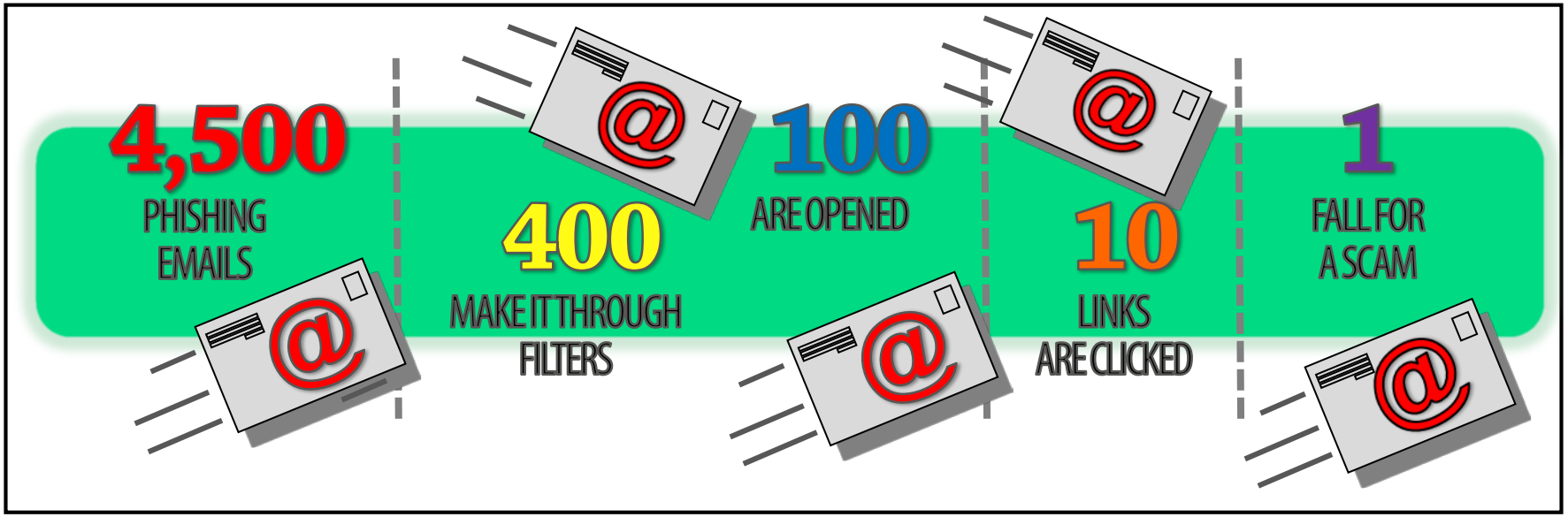
The Dridex Trojan has undergone a major version upgrade, releasing v4 and launching it in infection campaigns in the wild. Its main capabilities include stealthy account and device takeover, such as:

- Browser hijacking
- Credential theft
- Web injections for transaction manipulation and social engineering
- SMS-hijacking mobile component (via an Android app)
- Use of RAT to further control infected machines
- Screen capture sending images to the attacker's server

PHISHING – YOUR STAFF NEED TO BE ALERT TO THE EXTENT OF THE PROBLEM

LLOYDS BANKING GROUP

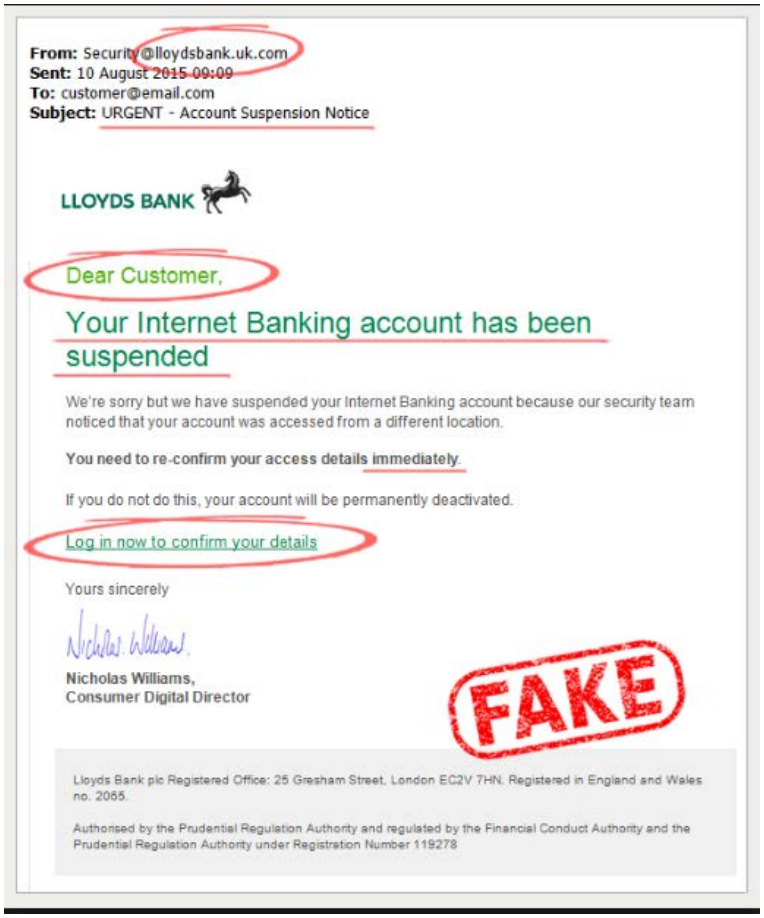
Malware contained with phishing emails is the most common distribution method.



- Distribution also via malvertising; external media devices; macros
- Quality of cyber security, hygiene and ongoing critical patch management
- Staff awareness, training and testing. Repeat, repeat, repeat!

SPEAR PHISHING EMAIL IS A COMMON MALWARE DISTRIBUTION TACTIC

Staff being alert to the threat and not clicking on links or attachments is a vital defence.



From: Security@lloydsbank.uk.com
Sent: 10 August 2015 09:09
To: customer@email.com
Subject: URGENT - Account Suspension Notice

LLOYDS BANK

Dear Customer,

Your Internet Banking account has been suspended

We're sorry but we have suspended your Internet Banking account because our security team noticed that your account was accessed from a different location.

You need to re-confirm your access details immediately.

If you do not do this, your account will be permanently deactivated.

Log in now to confirm your details

Yours sincerely

Nicholas Williams,
Consumer Digital Director

FAKE

Lloyds Bank plc Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales no. 2065.

Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under Registration Number 119278

PROMPT PATCH MANAGEMENT IS CRUCIAL!

Release of patch updates will be exploited by criminals with large scale malware distribution campaigns.

GET IT UPDATED!

ORGANISED FRAUDSTERS HAVE TIME TO RESEARCH FULLY BEFORE THE ATTACK

This gives them a real upper hand in being able to trick unwitting victims.

- Social Engineering techniques used to obtain confidential information – phone calls, phishing emails
- Which software product versions are you using? E.g. Word 2010
- Social media researching key officials
- Trading partners/supplier/ contractor information
- Financial information

SCAMSPOTTING

Video by the students of Sheffield University

https://vimeo.com/208179201

LAUNCHING THE ATTACK

Vishing, Invoice Fraud, Business Email Compromise (CEO Fraud) & Ransomware

VISHING (TELEPHONE SCAM) - A SIGNIFICANT THREAT TO ALL INDUSTRY SECTORS

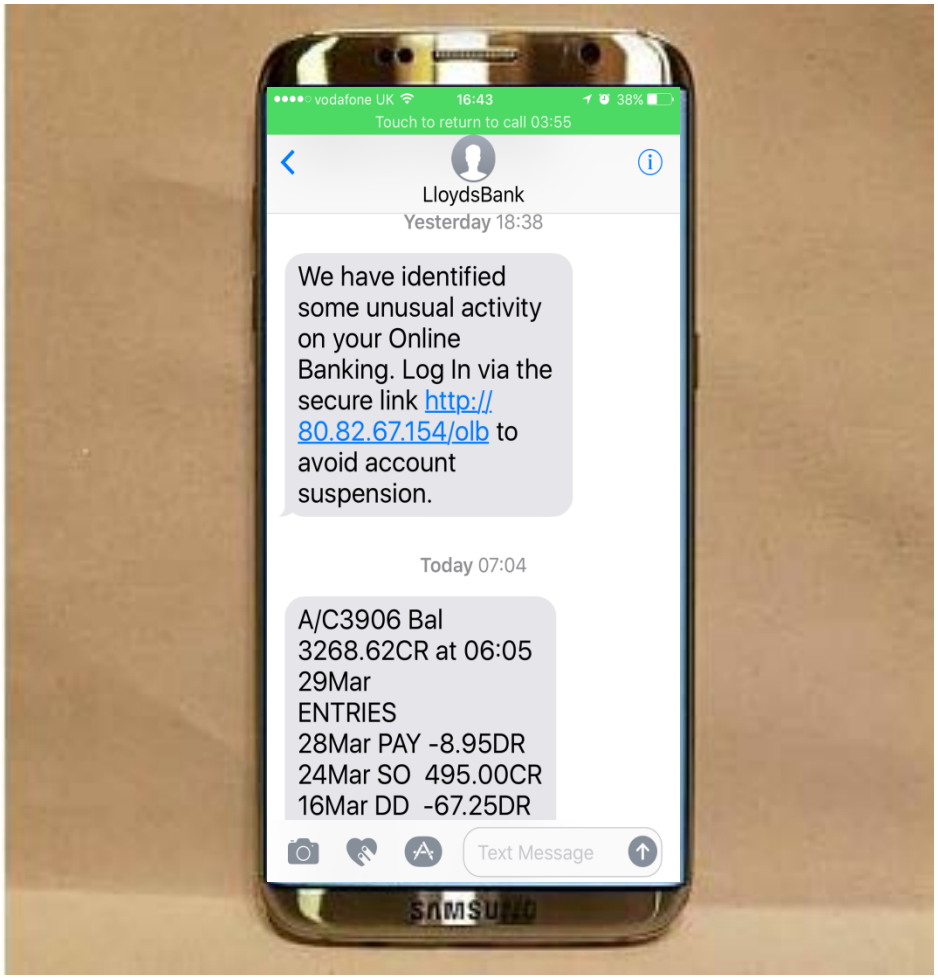
Payment clerks and teams are targeted and tricked into taking action under the misapprehension that they are protecting the organisation's money.

- Their objectives
- Savvy calls
- Techniques used
- Finding the money
- Successful Industry and Police collaboration – disruption

Social Engineering - Telephone Scam

SMISHING (SMS SCAM) IS A RECENT TYPE OF FRAUD TARGETING UK ENTITIES

The fraudsters objective is to harvest credentials to be able to access the victim's bank account.



RANSOMWARE HAS INCREASED EXPONENTIALLY IN THE PAST 12 MONTHS

It's proving to be a very lucrative and attractive fraud type attacking businesses across all sectors and sizes.

No guarantee if the ransom is paid

Visit 'No More Ransom!' website

Disruption caused by the need to forensically clean or rebuild system

HAVING A RANSOMWARE PREVENTION STRATEGY IS VITAL

A robust contingency plan will help avoid your business having to face the dilemma of deciding whether to pay the ransom or not.

- No guarantee of recovery if the ransom is paid
- Back up your files regularly to an independent source
- Update applications and operating systems
- System/application access – point of least privilege!
- Forensic cleansing required post incident & prior to running data recovery

RANSOMWARE STRATEGY

Summary risk management approach.

INVOICE FRAUD AND BUSINESS EMAIL COMPROMISE (CEO) FRAUD

These types of fraud are very lucrative.

Invoice Fraud accounts for:

35% of reported fraud losses borne by business customers.

Business Email Compromise (CEO) Fraud accounts for:

35% of reported fraud losses borne by business customers.

SIGNIFICANT INCREASE IN BUSINESS EMAIL COMPROMISE/CEO FRAUD

Police issue warning asking all UK businesses to be on alert.

- Impersonation by hacking into or spoofing a business owner or senior executive's email account.
- Instruction to invoice clerk or payments team. Urgent payment to specified account.
- Take advantage of employee's instincts of trust, fear and obedience.
- Replicating terminology the sender would ordinarily use.
- Unable to contact the sender to verify.

MANDATE/INVOICE SCAMS

Mandate/invoice scams are very active frauds targeting all industry sectors.

- Instruction from supplier to change bank account details.
- Research and pre-attack phone calls to add legitimacy.
- Build trust/relationship with the invoice clerk or Finance team.
- Redirection of all future payments. Delay before fraud is discovered.
- Time to move the money. Slim chance of recovery.

EMAIL INTERCEPTION COMPROMISING ELECTRONIC INVOICES IS EMERGING

Intelligence to date indicates activity initially instigated by West African fraud ring compromising businesses domiciled in the Far East is spreading.

- Email system compromise. SMTP DNS poisoning.
- Attacker monitors email traffic looking for pre order correspondence.
- Email between buyer and seller containing invoice intercepted.
- Beneficiary bank account details altered.
- Spoofs seller/vendor email address to send amended instruction.

RECOMMENDED SENIOR MANAGEMENT APPROACH TO FRAUD PREVENTION

FRAUD PREVENTION – ADOPTING A LAYERED APPROACH IS STRONGLY RECOMMENDED

It's prudent to work on the premise that one layer will be circumvented.

THERE ARE 5 KEY FRAUD PREVENTION TIPS

All business leaders are recommended to consider implementing the following measures if not already fully embedded.

- Be proactive, clear procedures.
- Review hiring procedures – infiltration
- Train employees in fraud prevention. Refresh regularly. Take 5!
- Implement a fraud hotline
- Set the tone – zero tolerance

KEY INFLUENCES ON THE FRAUD OUTLOOK

THE FUTURE FRAUD THREAT IS LIKELY TO CONTINUE TO INCREASE

This in part will be driven by new opportunities.

- Mobile Malware
- Crime as a service
- Data breaches – continued high profile events
- IOT
- New payment technologies
- Regulation

WHERE TO GO FOR FURTHER INFORMATION

EDUCATING YOUR STAFF

There is some excellent information available that can be used to help educate your staff.

- Lloyds Bank & Bank of Scotland websites

  lloydsbank.com/fraud
  bankofscotland.co.uk/fraud

- Webcast recordings

- Websites:

  Get Safe Online
  Action Fraud
  Take Five

- Cyber Essentials

- Bank Relationship Manager

QUESTIONS?

THE ‘TAKE FIVE’ CAMPAIGN PROVIDES VERY PRACTICAL FRAUD PREVENTION TIPS

It is strongly recommended that all employees are familiar with these basic principles.

- Never disclose security details such as your PIN, Full Password or Card/Reader codes
- Don’t assume an email request or caller is genuine
- Don’t be rushed - a supplier or genuine organisation won’t mind waiting to give you time to stop and think
- Listen to your instincts
- Stay in control

THANK YOU

Vin Pandha, Commercial Fraud Manager

vin.pandha@lloydsbanking.com

The Academies Accounts Direction for 2017 and Looking to the Year Ahead From A Financial Perspective

Robert Anderson
Partner

Email: randerson@streetsweb.co.uk

Agenda

- Sector Overview
- Guidance Update
- Other Key Issues

Sector Overview

	2016		2017	
Primary	3,046	19%	3,961	24%
Secondary	2,023	66%	2,146	70%
Special	178		226	
Alternative Provision	55		65	
	5,302		**6,398**	
Free Schools	304		347	
Studio Schools	40		36	
UTCs	39		51	
	5,685		**6,832**	

Sector Overview

Number of entities	01.08.2015	01.06.2017
SATs	1,995	1,812
MATs	861	932
	2,856	2,744

75% of MATs have 2 – 5 schools

Audited Accounts

- 93% of Accounts submitted on time
- 211 not submitted on time
- 120 included an emphasis of matter
- 110 related to going concern
- 46 qualified
- 8 outstanding

Regularity

133 modifications

Main areas include:

- Internal control weaknesses
- Internal financial reporting
- Procurement/tendering
- Independent checks of controls
- At cost policy

Management letter points

- Overall coming down
- Average of 4.5 per trust

Annual Accounts Return

Received on time	2,766
Received late	210
Non returners	37

Guidance Update

- Revised Timetable
- Academies Accounts Direction
- Academies Financial Handbook

Revised Timetable

Return Name	Submission Date
FMGS Return	Within 4 months of becoming an academy
Alternative Assurance Return	Within a month of Trust Joining a MAT
Budget Forecast Return Outturn	By 19 May 2017
Budget Forecast Return	By 28 July 2017
Land and Building Return (new)	**By 31 October 2017**
2016/2017 Financial Statement and Management Letter	By 31 December 2017
August 2017 Accounts Return	**By 19 January 2018**
Submission of the 2016/2017 financial statements of Companies House	By 31 May 2018

Academies Accounts Direction

- Academies cannot defer financial statements
- Financial instruments in accounting policies
- Small company filing options not available
- Enhanced pension disclosure
- Equality Act Regulations
- Information of the apprenticeship levy
- Teaching Schools should not be funded by GAG

Academies Accounts Direction

Accounting for church schools

- If existence of control, do not recognise
- Rent if can be reliably quantified
- Ensure disclosure

Academies Accounts Direction

Transfer issues

- Additional disclosure in accounts
- Agreement between trusts
- 4 month submission for SAT

Other Key Issues

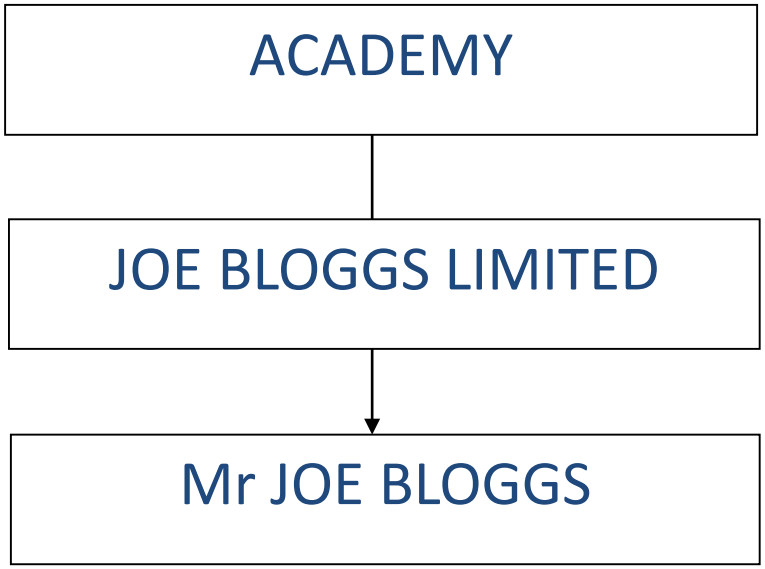
- IR35
- Going Concern
- Management Accounts
- Fraud

Off Payroll Working in the Public Sector (IR35)

Jennifer Taylor
Assistant Tax Manager

Email: jtaylor@streetsweb.co.uk
Telephone: 01522 551200

Off Payroll Working in the Public Sector (IR35)



Off Payroll Working in the Public Sector (IR35)

- Applies to payments made to contractors after 6 April 2017
- Tackles workers who would be considered employed if not for an intermediary
- Payments to deemed employees must be made through payroll and employment taxes deducted

Off Payroll Working in the Public Sector (IR35)

- Does the worker have to report to a manager who supervises their work?
- Is the worker entitled to choose their hours of work?
- Is the worker presented as a member of the school? E.g. School email address

https://www.gov.uk/guidance/check-employment-status-for-tax

Off Payroll Working in the Public Sector (IR35)

- Part-time teachers delivering the national curriculum
- Workers in managerial roles

Off Payroll Working in the Public Sector (IR35)

Jennifer Taylor
Assistant Tax Manager

Email: jtaylor@streetsweb.co.uk
Telephone: 01522 551200

Going Concern

- 60% of secondary schools running a deficit
- 3 -5 year forecasts
- Reserves Policy
- ESFA assistance – financial health and efficiency

Management Accounts

Outcomes of FMGS audits

"Financial reports presented to finance committee are often basic and not appropriate management accounts"

Management Accounts

Includes

- Results to date
- Budget
- Variances, including explanations
- Balance Sheet
- Evidence of challenge by trustees

Management Accounts

Balance Sheet

- Is cash decreasing unexpectedly
- Are trade creditors increasing
- Are debts not being recovered/potential bad debt

Fraud

AFH

- Have regard to risk, fraud and theft
- Accounting officer personal responsibilities
- Aware of risk, address risk, proportionate controls
- Responsible for taking appropriate action
- Above £5,000 = report to the ESFA

Fraud - Real Examples

- Loss of data
- Fake email from Trustee enclosing invoice
- Fake email from CEO requesting bank transfer

The Academies Accounts Direction for 2017 and Looking to the Year Ahead From A Financial Perspective

Robert Anderson
Partner

Email: randerson@streetsweb.co.uk