COMMERCIAL BANKING

Fraud risk

How exposed are you? At Lloyds Bank we want to help our clients stay safe from financial fraud. This brochure provides some guidance on the different types of fraud and how to protect your business.

LLOYDS BANK

An introduction

A message from our director

At Lloyds Bank Commercial Banking we are passionate about supporting our business clients and one of our key priorities is to help our clients stay safe from financial fraud. This booklet provides details of the latest scams impacting UK businesses and some very relevant ideas on how to avoid becoming a victim to financial fraud.

I lead a team of specialists across Fraud, Investigations, Financial Crime, Sanctions and Anti-Bribery and am very aware that fraud and cyber related fraud is on the rise, and that all businesses are vulnerable. It is essential that business leaders take the threat seriously and understand how they can reduce their business exposure.

In particular, impersonation fraud is on the rise in the UK and globally. Financial Fraud Action UK claims that "impersonation and deception scams continue to be one of the primary drivers behind business losses to financial fraud". In many cases where impersonation fraud takes place a cyber security attack may have occurred. The cyber breach can help fraudsters to conduct reconnaissance, research and harvest valuable information which is used to make their attack very convincing.

Please take some time to study this booklet and share it with everyone in your business who has a responsibility for making or authorising payments on behalf of the business. Afterwards, do take time to view our website for more information, details are provided further in this booklet.

Regards

Mark

Mark Brotherton, Director, Fraud & Financial Crime,
Lloyds Banking Group, Commercial Banking

ⓘ

15 year high

Fraud in the UK hit its highest level in 15 years in 2017*.

*Source: http://www.cityam.com/278761/business-fraud-uk-hits-15-year-high

Contents

Social engineering

The use of deception and manipulation to obtain confidential information or taking specific action

What is social engineering?

Social engineering is the manipulation of individuals into performing actions or divulging confidential information. Fraudsters use social engineering tactics because it is usually easier to take advantage of your natural instinct to trust than it is to find ways of breaking into your systems. This could be persuading you to provide passwords and PINs or to transfer money.

The types of social engineering attacks currently being used by fraudsters to dupe businesses include phishing, vishing, smishing and spoofing – more on this later.

Your social media footprint

Social media has become a valuable tool for fraudsters in carrying out social engineering attacks because of the wealth of information that can be found on a victim. Fraudsters will often use personal information contained on social media platforms to target employees of a victim business by purporting to be a trusted person and encourage them into disclosing confidential information or to take specific action e.g. send a payment.

What is spoofing?

Spoofing is when a fraudster imitates genuine telephone numbers or the email addresses of financial institutions or other trusted people or organisations.

For example, the fraudster may alter the incoming number that appears on your phone's caller display, to one that you know is the genuine number for the Bank. Alternatively, they could send an email that appears to come from a senior person within the business, instructing an urgent payment to be made, usually via online banking; however the senior person's email account is either hacked or copied by fraudsters

Implement a social media policy which helps employees understand their responsibilities when using social media both at work and at home

For further support, please visit: **www.getsafeonline.org/business**

Protecting your business from social engineering

Take five to stop fraud

Financial Fraud Action UK Ltd (FFA UK) urge you to Take Five to stop and consider whether the situation is genuine. Is this making sense?

1. **Never disclose security details, such as your PIN or full banking password**

   Banks and other trusted organisations will never ask you for these in an email, on the phone, by text or in writing.

2. **Do not assume an email or phone call is authentic**

   Just because they know your basic details, it does not mean that they are genuine.

3. **Do not be pressured into a decision**

   Under no circumstances would a bank or organisation force you to make a financial transaction on the spot.

4. **Listen to your instincts**

   If something feels wrong, it is usually right to question it. Fraudsters may appear trustworthy, but they may not be who they claim to be.

5. **Stay in control**

   Have the confidence to refuse their requests, especially if you feel that you are not in control.

www.financialfraudaction.org.uk

Online Fraud

Cyber enabled fraud

What is malware?

Your systems can be infected by malware (malicious software) through viruses and Trojans which can then interrupt your online banking sessions and present you with a fake, but seemingly genuine, screen prompting you to enter passwords and codes which can be captured. Fraudsters will use this information to access your online accounts and make fraudulent payments.

Protecting your business

- Protect all PCs and devices with anti-virus software
- Install software updates as soon as they are available
- Ensure unique, strong and secure passwords are used. Change often
- Only download software from verified and trusted sites
- Train all staff in online fraud awareness.

How does malware download to your systems and devices?

Malware code is often hidden in attachments, links and free downloads. Criminals are always looking for different ways of downloading malware and malvertising is one of the methods that is used. Malvertising uses unprotected online advertising to spread malware and involves injecting malicious or malware-laden code into advertisements on legitimate online internet site advertising networks and web pages.

Phishing is a key tool for malware to be downloaded onto your system.

See more about this on the next few pages.

> Research conducted for Get Safe Online Week revealed that almost 1 in 10 people in the UK has been a victim of a phishing fraud. That's a lot of people. A crucial way to protect yourself is to not click on links or open attachments if the source isn't 100% known and trustworthy, take your time and think twice, because everything may not be as it seems.

Tony Neate
CEO of Get Safe Online

Phishing emails

A seemingly genuine email designed to trick you into following its instructions

What is phishing?

Phishing is an email scam designed by fraudsters who masquerade as your bank or another trusted organisation to obtain confidential information such as personal information, bank details and passwords. Often the email will link through to a fake website and it may appear almost identical to the legitimate website. Additionally, the email communication will usually suggest that you must act urgently, maybe to prevent your online access from being blocked.

Remember, phishing emails can look extremely convincing by copying branding and spoofing email addresses to seem genuine.

Protecting your business

- Protect all PCs and devices with anti-virus software and install updates as soon as they are available
- Set up effective and on-going staff awareness training and testing
- Implement a supportive process so that phishing emails can be reported - early reporting means that quick action can be taken to reduce that risk exposure.

A case study: How does phishing work?

999 Doctors Surgery* receives an email from the bank advising them of upcoming improvements to their online banking service. It asks them to log-on, re-validate their security details and register new security questions. The email 'helpfully' provides a link for 999 Doctors Surgery to use.

A staff member follows the link which appears to take them to their online banking homepage. They enter the confidential security information that the screen asks for.

Unfortunately, although the sender's email address had Lloyds Bank within the name, the full email address was not genuine and was from a fraudster. By following the link to a fake site, 999 Doctors Surgery has now given the fraudster information that they may be able to use to access their online banking.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

How to avoid a phishing scam

Best practice

1. **Think before you click**

   Beware of clicking on links or opening attachments contained in emails. Hover the mouse over the link and the URL details should come up and show if it is genuine. Ensure that the email address fully matches the trusted organisation's email address.

2. **Be wary of emails asking for confidential information**

   The bank will never email you asking you to disclose passwords or any other sensitive information.

3. **Open up a new web page in your browser and go to the website independently rather than clicking on an email link**

   A link within a phishing email could result in a virus or malicious software (malware) being downloaded onto your machine which the fraudsters will use to steal things such as your account details and data.

4. **If suspicious - contact the sender directly**

   Do not use the contact details or links provided in the email or reply to the email.

5. **Use a SPAM FILTER on all your email accounts**

   If you spot a suspicious email mark it as spam and delete it immediately without clicking on any links or attachments.

6. **Other key signs**

   Things such as the spelling and grammar are of poor quality, including graphic designs and images.

   Email is addressed to ‘Dear Customer’ for example where you hold a standing relationship with this organisation and previous communication has been addressed to you directly.

Ransomware

Malware extortion attack

What is ransomware?

Ransomware is a growing threat to businesses of all sizes and across all sectors

This is a type of malware that operates by blocking access to key files typically by encryption, which requires a private key to decrypt files and restore your access. An attack is followed with a ransom demand to restore your access to the files and documents. The ransom payment is usually requested by digital currency e.g. Bitcoin which is almost impossible for the authorities to trace.

Businesses of all sizes and across all sectors are targeted.

Visit 'No More Ransom' website for information on how to prevent this type of Fraud:

www.nomoreransom.org

Protecting your business

- Ensure all PCs are protected by high-quality antivirus software, keep your firewalls switched on and run frequent scans
- Always ensure updates are actioned promptly. These updates will often contain important security upgrades which will help protect your devices from viruses and hackers
- Make sure staff are trained in online fraud awareness and understand the importance of not opening any files attached to an email from an unknown, suspicious or untrustworthy source
- Backup all of your important data to an independent source such as an external hard drive or an online backup service.

A case study: How does ransomware work?

Jayne's PC at ABC School* displayed a message which stated that all of the data on the computer had been encrypted and it demanded a ransom of £500, payable in Bitcoin, for an encryption key.

The message stated that the encryption key will be destroyed at a set time within a short period, therefore Jayne and the organisation had a short timescale to act. The school decided not to pay the ransom, but because the data had not been backed up for 2 weeks the school lost that data and had to spend time reconstructing it.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

> “The ‘remorseless’ growth of cyber crime is leading to 4,000 ransom attacks a day”
>
> **Head of Europol**

Source: http://www.dailymail.co.uk/sciencetech/article-5063313/Fast-growing-cyber-crime-threatens-financial-sector-Europol.html#ixzz55gAC3mS8

Vishing & Smishing

Social engineering methods

What is vishing?

The largest frauds we have seen to date are as a result of vishing. Vishing is a telephone scam, usually to trick you into providing online banking passwords, confidential details or to persuade you to transfer money from your account.

Fraudsters, often purporting to be from your bank's fraud department, may call you to report a problem with your account and ask you to confirm that payments are genuine or ask you to move money into a 'safe account'.

Often, through the research carried out, the fraudsters will have your name, address, colleague names and bank details—essentially the kind of information that you would expect a genuine caller to have. Additionally, the fraudster will create a state of urgency and inform you that your money is at risk and that you have to act quickly, creating fear that no action will lead to a financial loss.

What is smishing?

Smishing targets the users of mobile phones using text messages to obtain private and confidential information from individuals or encouraging them to ring a number or click on a link for more information.

The message will typically alert you to a problem with your account. Fraudsters may spoof (see p4) the message onto a genuine message thread.

Protecting your business

- Take care if divulging confidential or personal information over the phone, text or email even if it seems genuine
- Verify the identity of the person/entity contacting you. Contact the company on a public number that is TRUSTED and VERIFIED
- Remember, the Bank will never ask for your online login details on the phone and will never ask you to move money to a 'safe' or 'secure' account.

A case study: How does vishing work?

Builders Limited* receive a phone call purporting to come from the bank stating that their account has been targeted by fraudsters and they need to take immediate action. The phone number displaying on the incoming call shows a number known to match that of the bank.

They are given information that leads the building firm to believe that the call is genuine. They are advised to move all funds (£250,000) to a 'secure' account, which they do following instructions. The next day they contact the bank and realise the call was not genuine. They had been tricked into sending £250,000 to an account at another bank under the fraudster's control. When contact was made with the bank who received the funds they advised that all monies had been transferred into accounts at multiple banks. Only £27,000 was recovered for the building firm.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

CEO Fraud

A fraudster assuming the identity of a senior member of your business

What is CEO fraud?

CEO fraud continues to be an active fraud threat.

This is where fraudsters send an urgent email payment instruction to a member of staff within a business and make it look like it has come from the genuine CEO of the company or another senior person. They do this by spoofing the email address or setting up an almost identical email account name or sometimes hack the CEOs email account.

Small and large organisations alike have been targeted and fallen for the scam.

Organised fraudsters often carry out extensive research on their potential victims, using information gleaned from malware and social media to lend credibility to their scam by using terminology and language that the sender would ordinarily use and timing the request to coincide with the alleged sender being unavailable e.g. on holiday.

Protecting your business

- Implement a clear structure for how payments should be made e.g. dual-authentication
- Create a culture that allows any member of staff, senior or junior, to challenge and verify payments through a clear, well documented policy
- Establish procedures that direct staff in what to do if they have made a suspicious payment instruction – quick action can contain losses
- Raise staff awareness of the current scams on a regular basis.

A case study: How does CEO fraud work?

Sarah, who is the finance director for Adjacent PLC*, received an email from her Chief Executive Officer, Jane, requesting an urgent payment of £85,000 to secure a contract with an important client. Additionally, the email stated that since Jane is on holiday she doesn't want to be disturbed with work matters. The email stated that there is a sensitive nature of the transaction and it requires strict confidentiality.

Sarah, knowing that this is a common occurrence, failed to check for the proper signs of fraud and followed the instructions sent to her by who she thought was Jane. She sent the payment and sent a separate email to Jane stating that the payment was complete. Jane immediately rang and questioned the payment. Jane had never requested such a payment, it was fraudulent. Sarah immediately informed her bank that this payment was fraudulent. The early reporting by Sarah meant that £50,000 was recovered.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

Invoice Fraud

Fraudsters impersonating a regular supplier or contractor

What is invoice fraud?

Fraudsters contact a business posing as one of their suppliers, contractors or clients and they request that future payments are sent to a different bank account.

Usually they claim to be a regular supplier who has recently changed their bank account details. The fraudster sends the business new details (sometimes on headed note paper) advising of changes to the supplier's bank account. The details are amended by the business, who believe that any funds remitted will still be transferred to the original beneficiary. However, when the next payment is sent, the funds are actually sent to the fraudster's account.

Protecting your business

- Establish a single point of contact (SPOC) with companies to which you make regular payments
- Always verify the source of any change of details requested, EVEN PHONE NUMBERS, by using a confirmed and recognised telephone number or with your usual contact or SPOC
- Have a clearly documented procedure so that all staff know how to handle any requests to change details and make sure that they know where the procedure is recorded
- Raise awareness with all staff, alerting them to this fraud type and test them regularly.

A case study – How does invoice fraud work?

XYZ Building PLC* regularly purchases materials from ABC Merchants*.

A fraudster sent a letter to XYZ on what appeared to be ABC Merchants' headed paper. It advised that ABC had changed their bank account, quoting a new sort code and account number for all future payments to be sent to.

XYZ amended the account details held for ABC in their payment records. When ABC sent the next monthly invoice of £60,000 for materials supplied, XYZ authorised payment to the new account.

The £60,000 was sent to the new account controlled by the fraudster. ABC contacted XYZ chasing non-payment, at which time the fraud was discovered and the funds long gone.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

> Verify changes of instruction using a known contact or independently sourced telephone number

Senior manager
Fraud and Financial Crime
Lloyds Banking Group

Cheque overpayment

Advance payment scam

What is cheque overpayment?

This is a common scam that is targeting businesses of all sizes.

This is where a fraudster purporting to be a new customer contacts you to order goods or services. Whilst the fraudster will lead you to believe that the payment will be transferred into your account electronically and ready for immediate use, it will actually be a counterfeit or stolen cheque that will be credited. The cheque will be made out for much more than the value of goods or services purchased. Following the payment, the fraudster will dupe you into urgently processing the refund for the overpayment.

The fraud is only discovered when the stolen/counterfeit cheque is returned unpaid but by that time you have paid the fraudster 'the overpaid' amount and are now left out of pocket.

Protecting your business

- Be suspicious of any new clients who send a larger amount of funds than you were expecting
- Ask the Bank to check the origin of any such overpayments before returning the money
- Check with the Bank to know whether a cheque has definitely been 'paid'.

A case study – How does cheque overpayment work?

Alpha Limited* receives an order for £2,000 worth of goods from a new client. The client promises to send an online payment so the goods can be dispatched. When Alpha check their bank account they find a payment for £20,000. They contact the client who says the overpayment is a processing error.

The new client asks for Alpha to return the extra £18,000 to a specific bank account. Alpha returns the £18,000 using online banking and dispatches the parts for the original £2,000 order.

A few days later Alpha realise that the £20,000 payment was actually a cheque paid in at a branch counter and has been returned unpaid. They have lost £18,000 in cash and £2,000 worth of goods. They contact the bank immediately for help, but unfortunately £12,000 had been moved out and was unrecoverable.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

Employee Fraud

Fraud committed by an employee or book-keeper

What is employee fraud?

Internal or employee fraud is when fraud is committed against the company or organisation a person is working for.

There are a number of ways in which employees or contractors can commit fraud against their employers and include falsifying expenses claims, misappropriating assets and making financial payments drawn on the business for personal gain.

Employee fraud has escalated recently across the UK and the risks that are involved can have serious consequences for businesses across all sectors and sizes. The costs of dealing with this type of fraud are high and the chance of retrieving lost money is slim.

Protecting your business

- Implement a robust recruitment process, including criminal record and character checks for applicants
- Regularly review employee access to business bank accounts, telephony and Internet passwords and to your computer systems and files. Restrict access to only those who need it
- Treat cheque books and cards with the same level of security as cash
- Ensure employees dealing with business finances are adequately supervised by senior colleagues. Have open conversations with employees and publicise the steps taken against fraudsters to show that fraud is not tolerated
- Have a strong whistleblowing reporting facility to allow employees to report suspicious activity anonymously.

Where to find out more:

www.actionfraud.police.uk

www.cyberaware.gov.uk

www.getsafeonline.org/business

Card and Cheque Fraud

Understand the common risks

Cheque fraud

What are the risks?

Criminals can target your business by printing counterfeit cheques to take money from your account. They can steal genuine unused cheques or chequebooks, then forge your signature. Or they can fraudulently alter cheques you have written by changing the payee name or, if they are the payee, by increasing the amount that's payable to them.

Protecting your business

- Complete cheques fully before signing and cross through spaces on your cheques after the payee name and amounts
- Write payee names in full e.g. "Lloyds Banking Group" rather than ' LBG or Lloyds'
- If you issue cheques using a laser printer, use one recommended for cheques
- Keep cheque books secure and reconcile cheque payments to statements reporting inaccuracies immediately
- If you are expecting a new cheque book, contact us as soon as possible if it does not arrive.

Card fraud from the user's perspective

Protecting your business

- Ensure you are the only person that knows your PIN – banks or the police will never ask for it
- Watch out for card expiry dates. If your replacement card doesn't arrive, call the bank
- If you move your business correspondence address, tell your bank, card issuer and other organisations that you deal with straightaway. Ask the Royal Mail to redirect your post
- Always shield the keypad to prevent anyone seeing you enter your PIN. If you spot anything unusual about the cash machine don't use it – report it to the bank concerned immediately.

On the Internet

- Protect your PC with the latest firewall browser and antivirus software
- Look for the padlock symbol when buying online – it shows the information you input will be encrypted.

Card fraud from a merchant's perspective

Protecting your business if you need to accept payments made by card:

- Consider 3D secure for processing card payments – it offers greater protection from fraudulent payments
- Ensure your business has sufficient staff who know how to review high risk transactions referred by your merchant services supplier
- Chip & PIN terminals must be held securely at all times to avoid unauthorised tampering
- Any cardholder information must be held securely and in accordance with the card payment industry requirements. Access to this information should be restricted only to those staff needing it
- Comprehensive security information will be available from your merchant services provider. Ensure that all key staff are aware of the security guidance.

Our service promise. If you experience a problem, we will always try to resolve it as quickly as possible. Please bring it to the attention of any member of staff. Our complaints procedures are published at **lloydsbank.com/business/contactus**

Lloyds Banking Group is committed to protecting our customers. If you have any concerns or need some support with understanding the information in the brochure you have just read, due to your personal circumstances, please contact your relationship management team. We will do all we can to help you understand the content of this brochure.

I'd like to find out more

- Go to lloydsbank.com/fraud
- Contact your relationship management team

Please contact us if you would like this information in an alternative format such as Braille, large print or audio.

If you have a hearing or speech impairment you can use the Next Generation Text (NGT) Service (previously Text Relay/ Typetalk) or if you would prefer to use a Textphone, please feel free to call us on 0345 601 6909 (lines open 7am-8pm, Monday-Friday and 9am-2pm Saturday).

Important information

Calls may be monitored or recorded in case we need to check we have carried out your instructions correctly and to help improve our quality of service.

Lloyds Bank plc Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales no. 2065. Telephone: 0207 626 1500.

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

Eligible deposits with us are protected by the Financial Services Compensation Scheme (FSCS). We are covered by the Financial Ombudsman Service (FOS). Please note that due to FSCS and FOS eligibility criteria not all business customers will be covered.

Lloyds Banking Group is a financial services group that incorporates a number of brands including Lloyds Bank. More information on Lloyds Banking Group can be found at lloydsbankinggroup.com.

LLOYDS BANK