
COMMERCIAL BANKING
FRAUD GUIDANCE
Helping you to protect yourself
LLOYDS BANK

In the UK more than 40% of businesses have experienced fraud in the last year with an average loss of £4,515.

To help you protect yourself and your business we've created this guide with some key actions to take.

Taking some very basic steps can make a real difference to fraudsters' success rates.

SUPPORT

CHEQUE FRAUD

The illegal use of cheques to acquire funds.

CHEQUE FRAUD

HOW CAN CHEQUE FRAUD AFFECT YOUR BUSINESS?

Cheque fraud can happen in a few different ways. Criminals can steal cheques, create fraudulent cheques or change the name or amount on a legitimate cheque.

The following are the main types of cheque fraud:

Counterfeit cheques are copy cheques, printed to look exactly like your genuine cheques. A fraudster may use these to try and take money out of your accounts.

Forged cheques are genuine cheques that have been stolen and used by a fraudster with a forged signature, in an attempt to take money out of your accounts.

Fraudulently altered cheques are genuine cheques that you have written, but a fraudster has altered. Either the fraudster will intercept the cheque and alter it in some way before they try to pay it in e.g. by altering the beneficiary's name and/or the amount, or they will be the genuine payee but might try to increase the amount payable to them on the cheque.

There are also **cheque fraud scams** that fraudsters may use to attack your business.

A cheque you are not expecting, or for an amount more than you require, is paid into your account by a fraudster presenting himself as a genuine customer. The fraudster then asks for the overpaid funds to be returned. After you have done this, the cheque is returned as fraudulent.

Fraudulent cheques can be given to you as payment for high value goods. After you have released the goods. the cheque is returned as fraudulent.

CHEQUE FRAUD

WHAT ACTIONS CAN YOU TAKE TO PROTECT YOUR BUSINESS?

ISSUING CHEQUES:

Cross through spaces on cheques you issue. Eg. after the payee name and the amounts (words and figures).

Use a **printer** which is recommended for cheques, if they are issued using a laser printer.

Always use a black or blue ballpoint or a pen with **indelible ink** so that writing cannot easily be erased or altered. **Apply more pressure** with the pen tip than normal, to make the writing difficult to remove.

If boxed cheques are used, **enter ZERO** rather than NIL, which can be changed to NINE.

Write **full payee names** rather than acronyms. Eg: British Broadcasting Corporation rather than BBC.

CHEQUE FRAUD

WHAT ACTIONS CAN YOU TAKE TO PROTECT YOUR BUSINESS?

BEST PRACTICE:

- Consider whether cheque is the **best method** for the payment. Online payments, BACS, CHAPS can be faster and more appropriate.
- **Reconcile** cheque payments to statements and report inaccuracies immediately.
- Keep cheque books **secure.**
- Make sure cheques can‘t easily be recognised in the **post** – especially if window envelopes are used.
- If you are due to receive a **new cheque book,** contact us as soon as possible if it does not arrive.
- Look out for cheques that have been removed from the **middle or back** of your cheque book

FURTHER GUIDANCE AND HELP:

If you think you have been a victim of cheque fraud please report your suspicions to the Bank immediately.

Useful websites:

Action Fraud
Cheque and Credit Clearing Company

AVOIDING CHEQUE FRAUD SCAMS

Make sure the cheque has **definitely been “paid”** and that the funds are cleared in your account before releasing goods or returning any funds.

Do not accept cheques made payable for a higher value than you were expecting

CARD FRAUD

Plastic card fraud involves the compromise of any personal information from credit, debit or store cards

CARD FRAUD

HOW CAN CARD FRAUD AFFECT YOUR BUSINESS?

Fraudsters adopt a number of different approaches to obtain card and PIN details for illegal use.

The most common fraud types:-

Account Takeover is where a fraudster gains control of your card account and makes unauthorised transactions

False Application is when a fraudster opens an account using fake or stolen documents in your name

Card Not Present is when the fraudster makes transactions using card details via online, telephony or mail order.

Card Not Received is when the fraudster intercepts your card in the post and makes fraudulent transactions

Counterfeit cards are fake cards created by the fraudster.

Lost/Stolen cards resulting in a fraudster using your cards to make unauthorised transactions or payments

The most common card fraud is the use of compromised card details in 'Card Not Present' transactions e.g. internet, telephone and mail order purchases.

CARD FRAUD

WHAT ACTIONS CAN YOU TAKE TO PROTECT YOUR BUSINESS?

Using cards overseas

Only take cards that you intend to use; leave others in a secure place at home.

Make sure you have your card company's 24-hour contact telephone number.

Preventing Card ID Theft

Always keep important personal documents, plastic cards and cheque books in a safe and secure place.

Don't share personal information unless you are confident you know who you are dealing with.

Internet Fraud

Keep your PC protected. Ensure you have the latest operating system firewall browser and up to date Anti- virus software.

Look for the padlock symbol when making online purchases. It's an indication that the site is reputable and the information you input will be encrypted.

Always log out properly after shopping

Mail and Phone

Never leave your card or card details lying around or keep your card and PIN together. Never let anyone else use your card and never send a supplier a copy of the front or back of your card.

Only make telephone transactions when you have instigated the call and are familiar with the company.

Further information

The Action Fraud website provides excellent guidance on Credit Card Fraud and Debit Card Fraud

Using Cards at a Cash Machine

Always shield the keypad with your free hand and your body to avoid anyone seeing you enter your PIN.

If you spot anything unusual about the cash machine do not use it. Report it to the bank concerned immediately.

CARD FRAUD

WHAT ACTIONS CAN YOU TAKE IF YOUR CARD IS LOST OR STOLEN?

Ensure you are the only person that knows your PIN. Banks or the police will never contact you to ask you to disclose it.

The bank can arrange for you to collect valuable items such as new plastic cards or cheque books from a local branch if other people have access to your mail.

Pay attention to card expiry dates. If your replacement card hasn't arrived, call the bank to check the status of your new cards.

Contact the Royal Mail Customer Enquiry Line on 08457 740 740 if you suspect your mail is being stolen.
.

Tell the bank, card issuer and all other organizations that you deal with immediately, if you move your business correspondence address. Ask the Royal Mail to redirect any mail from your old address to your new one for at least a year.

ONLINE FRAUD

Some fraudsters rely on the internet to commit their crimes

ONLINE FRAUD

HOW CAN ONLINE FRAUD AFFECT YOUR BUSINESS?

Vishing involves fraudsters telephoning to obtain confidential information from you, usually asking for bank details and online banking passwords.

The call often starts with the fraudster advising you that funds held in your account have been, or are about to be stolen. You might be asked to call the bank back, using a number from the back of your bank card or bank statement. The fraudster holds the phone line open by not putting down the receiver at their end, so you unknowingly phone the number to only go back to speaking directly with the fraudster, who continues to mask them self as the bank. Victims are then told to transfer funds to a 'safe' account which has been opened for them. The account will be under the control of the fraudster.

Malware refers to malicious software such as viruses and Trojans. Malware is often hidden in attachments and free downloads. It can capture your keystrokes to see your passwords and then use them to access your online accounts.

The fraudster may use the malware to present seemingly genuine online banking log-on screens on your computer and they could then use any passwords that you enter into this screen, to potentially access your accounts.

Phishing occurs when fraudsters attempt to obtain your bank details, online banking log-on passwords, or other confidential information by masquerading as the bank or other trustworthy entity in an email.

The email will usually link through to a fake website, which looks almost identical to the bank's legitimate one. A message usually suggests that you need to act urgently, for example to prevent your online access from being blocked.

ONLINE FRAUD

WHAT ACTIONS CAN YOU TAKE TO PROTECT YOUR BUSINESS AGAINST VISHING?

If you are not **certain** that it is the Bank calling, call the Bank back using a **number known** to be correct, preferably using a different phone line (eg a mobile phone). If this is not possible ensure the phone line is clear first by waiting at least 5 minutes before calling back. Alternatively call a friend or family member first to test the line.

Never divulge online banking passwords to anyone.

Vishing callers often ask you to move funds from your bank account to **a "safe account"** (one which is controlled by the fraudster) – Lloyds Bank will NEVER ask you to move your funds to a safe account.

Remember, the Bank will **never ask** for online log-on details on the phone.

Vishing calls are often received at **night or at weekends**. Fraudsters know that victims may not immediately report their suspicions to the bank.

.

If you think you have been the victim of online fraud **please contact us immediately at:**

Lloydslink Helpdesk - 0870 900 2070
Online for Business Helpdesk - 0800 015 0082
Calls may be monitored or recorded. If you have a hearing or speech impairment you can use Text Relay (previously Typetalk). 0845 3002281

ONLINE FRAUD

WHAT ACTIONS CAN YOU TAKE TO PROTECT YOUR BUSINESS AGAINST MALWARE?

Where possible, consider having **more than one individual** required to set up and send each payment.

If your online security requires a **card and reader** to be connected to your PC, remove the card as soon as you have logged on and only re-insert to carry out a signing action.

Ensure that all PCs are **protected** by high quality anti-virus and anti spy-ware software, which is updated regularly and run regular scans to identify and remove malware

Check all **payment details** thoroughly when approving and releasing payments.

Take care when downloading programs to your PC. Is the website or link to be downloaded from a trusted source?

Always **log out correctly** when you have finished online banking. If a session ends unintentionally, always log-on again and logout correctly**.**

If any of the following are experienced, log-out of online banking **immediately** and if in use, remove any cards from readers connected to your PC and call the bank:

1. When connecting to online banking the PC runs unusually slowly, or has a continual spinning egg timer
2. The application presents unexpected screens, or pop up windows, or asks a user to repeat their log–on information.

ONLINE FRAUD

WHAT ACTIONS CAN YOU TAKE TO PROTECT YOUR BUSINESS AGAINST PHISHING?

Hover over any **links within emails**, to see what the true web address is.

Look out for emails which are poorly worded or have **incorrect spelling**.

Remember that genuine Bank emails will **contain your name** – be wary of anything that begins with 'Dear valued customer' or similar.

Use a **SPAM filter** to remove unwanted emails and when on websites, opt out of receiving future marketing emails.

Keep personal and business **information** stored online to a minimum and be careful around what information is added to networking sites

Bank emails should only ever contain a link to the Bank's Home pages.

We'll never send an email asking a client to enter log-on, account or personal details, or an email with a link to a page that requires this information.

Useful websites:

The Lloyds Bank Commercial Site has a section on **online services** and specific **security** pages for the online banking service you use.

Action Fraud

Government Cyber Streetwise website

Bank Safe Online

Get Safe Online

SCAMS

Fraudsters will adopt a number of different approaches to try and dupe businesses into parting with funds in their bank account.

FRAUDULENT INVOICE SCAMS

XYZ Building Plc* regularly purchases materials from ABC Merchants.

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

XYZ acted upon the request and amended ABC account details in their payment records held with their bank. ABC sent the next monthly invoice of £60,000 for materials supplied. XYZ instructed their bank to send the payment.

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

What you can do to protect your business:

Businesses should undertake a thorough review of existing processes for sending and receiving payments and ensure that there are strong authentication measures in place, to make sure payments are being made to the correct beneficiary.

Establish a single point of contact (SPOC) with each regular supplier.

Telephone suppliers via their verified company switchboard number and confirm any requests to change payment details with the SPOC.

CHEQUE OVERPAYMENT SCAMS

123 Parts Limited* has received an order from a new client for goods totalling £2,000. The new client promises to send an online payment so that the goods can be despatched. When 123 Parts Limited check their bank account they realise that the payment received is for £62,000. When they contact the new client, they are told that this larger amount was the result of a processing error.

The new client requests that 123 Parts Limited return £60,000 of the funds, to a bank account that the new client specifies. 123 Parts Limited returns the funds using online banking and dispatches the parts for the original £2k order.

A few days later they realise that the original £62,000 payment was actually a cheque paid in at a branch counter and has now been returned unpaid. 123 Parts Limited had now lost £60,000 in addition to £2,000 of goods. They contact the Bank immediately for help in recovering the funds and fortunately the funds still remained in the fraudsters account at another bank, with a full recovery made.

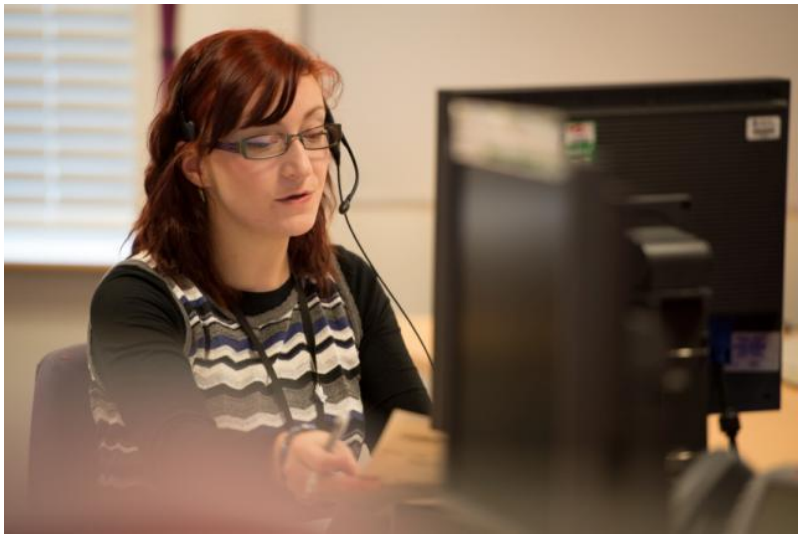
What you can do to protect your business:

Any new clients of your business, who send a larger amount of funds than you were expecting, should raise immediate suspicions.

Ask the Bank to check the origin of any such overpayments.

You should check with the bank if you need to know whether a cheque has been “paid”. A cheque that has purely “cleared” **can** still be returned.

PHISHING SCAMS



999 Doctors Surgery*, receives an email from the Bank instructing them that due to improvements to their online Banking Service they need to log-on to online banking, to re-validate their security details and register new security questions. The email “helpfully” provides a link for 999 Doctors Surgery to use.

They follow the link and are directed to a site which appears to be their online banking homepage. A member of staff from 999 Doctors Surgery enters their details and supplies confidential 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 which directed them to a fake site and entering their personal details, 999 Doctors Surgery has now provided the fraudster with information that they may be able to use to access their online banking.

What you can do to protect your business:

Remember that genuine Bank emails will contain your name – be wary of anything that begins with ‘Dear valued customer’ or similar.

Bank emails should only ever contain a link to the Bank’s home page. We’ll never send an email asking you to enter log-on, account or personal details, or an email with a link to a page that requires this information. Delete such emails, even if they look genuine.

Hover over any links within emails, to see what the true web address is.

VISHING SCAMS

ABC Agriculture Limited* receive a phone call from the Bank stating that their account has been targeted by fraudsters and their funds are at risk, unless immediate action is taken. They are advised to contact their Bank immediately using the telephone number from the back of their card, to secure their funds.

ABC Agriculture make a call to the number printed on their card. They are instructed to move all funds (£350,000) to a 'secure' account. ABC Agriculture follow the instructions and send the money to the 'secure' account.

The next day they contact the Bank and realise that the call was **not** genuine. The fraudster had impersonated the Bank. When ABC Agriculture had phoned the number from their statement, they had unknowingly continued the same call with the fraudster as the fraudster had kept the phone line open.

They had been tricked into sending £350k to an account at another bank, under the fraudster's control.

What you can do to protect your business:

If you are not **certain** that it is the Bank calling, call the Bank back using a number **known** to be correct, preferably using a different phone line. If this is not possible ensure the phone line is clear first by waiting at least 5 minutes before calling back, or by calling a friend or family member first to test the line.

Remember, the Bank will never ask for online log –in details on the phone and will never ask you to move money to a "safe" or "secure" account.

Be wary of calls received seemingly from the Bank, at night or at weekends. Fraudsters know that businesses may not report their suspicions to the bank at these times.

*The business names used in these case studies have been changed, to protect the identity of genuine clients.

EMPLOYEE FRAUD

Employee Fraud has escalated recently across the UK * and this risk can have serious consequences for businesses which are targeted.

*Source: CIFAS Fraudscape Publication

EMPLOYEE FRAUD

HOW CAN THIS AFFECT YOUR BUSINESS AND HOW CAN YOU PROTECT YOURSELF?

The most common means of obtaining money is by corrupt employees presenting cheques drawn on their employer's business account for personal gain, often forging signatures.

Given the high costs of dealing with employee fraud and the often poor prospects for the return of lost monies, a priority for any business should be a robust recruitment policy, aligned to the business type and risks. Businesses should also minimise the fraud opportunities, with robust and regularly reviewed controls.

Actions to be considered:

Have a robust recruitment process, including criminal record and character checks for applicants .

Ensure procedures that surround access to the business bank accounts, security of telephony/internet passwords and authentication credentials are reviewed regularly and check your bank statements regularly and thoroughly.

Treat cheque books and cards with the same level of security as you would treat cash.

Ensure employees dealing with business finances are adequately supervised and their activities are regularly monitored by senior colleagues. Have open conversations with employees. Publicising the steps taken against fraudsters, helps send a clear message that fraud is not tolerated.

What should you do if you fall victim to this fraud?

Contact us and tell us about the incident.

Your account manager can provide practical support in the following ways:

- Help to contain the extent of losses
- Help to secure and protect the bank account and records
- Provide support and assistance to recover funds lost to criminal activity
- Support the business internal investigations and any Police investigations
- Provide financial support, advice and guidance

VIRTUAL CURRENCIES

a type of unregulated, digital money
the use of which has grown
significantly in recent years.

VIRTUAL CURRENCIES

FACTS AND POINTS TO CONSIDER

A key consideration regarding virtual currency, is that it is not legal tender. ie not recognized by a legal system to be valid for meeting a financial obligation.

Virtual currencies are often traded in online marketplaces or gaming communities, but can be used to purchase real world products or exchanged for 'traditional' currencies. The most widely known virtual currency is Bitcoins, so for example X Bitcoins can be exchanged for X pounds or X Bitcoins can be used to purchase a product from an online retailer. Bitcoins are stored in a password protected Bitcoin digital wallet.

A decentralised currency is a "currency":

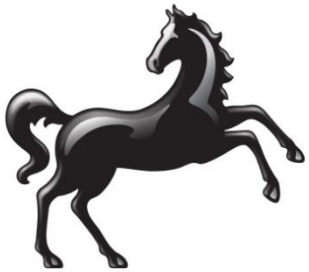
- that has **no central repository** and no single administrator
- that persons may **obtain** by their own computing or manufacturing effort
- that rather than relying on confidence in a central authority, depends instead on a distributed **system of trust**

Due to their de-centralised nature and lack of regulation, virtual currencies are particularly attractive to fraudsters wanting to launder criminal funds.

As the use of virtual currencies is still a relatively recent concept in terms of wider usage, the precise nature of some of the threats resulting from crime, are only just becoming known.

Virtual Currencies usually operate on a decentralised network that allows its users to transfer ownership of the currency from 'person to person'

Organised fraudsters have manipulated virtual currency markets in order to lower the value, enabling them to purchase in bulk, before driving the value up, so they can sell them on for profit.



LLOYDS BANK

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