

Fraud Awareness

By working together we can help to reduce fraudulent activity by making it difficult to undertake and easy to detect fraud at the earliest opportunity.

This information booklet will assist you to put in place the internal controls to assess, prevent and detect the risk of your organisation being affected by fraud.

The Cheque and Credit Clearing Company has released figures which show that cheque fraud losses have decreased from £29.8 million in 2009 to £28.9 million in 2010.

“The continuing drop in cheque usage has also contributed to the three per cent fall in overall cheque fraud losses” says Financial Fraud Action UK.

Although the majority of fraudulent cheques get stopped before the cheque is paid, by recognising potential process weaknesses and highlighting the need for strong internal controls and efficient reconciliation, you can successfully fight fraud.

The Bank will provide you with advice and guidance, however your organisation should still take appropriate independent advice on the management of fraud. Ultimately the responsibility is yours.

Prompt action will assist the Bank to recover your funds quickly

Check every statement against your own records. Should a discrepancy be found, please contact the Bank immediately by calling **0845 140 1000** or send an email to **fraud@unity.co.uk**.

Do you need to write a cheque out?

Always consider other methods of payment when dealing with large amounts. We offer a variety of services such as one-off Standing Order¹ payments or CHAPS² (there is a charge for these services). Alternatively you may wish to use Internet Banking where payments can be sent to any bank account via the Bill Payment³ service free of charge.

This facility is available to accounts which require more than one signatory. If you would like to discuss these options call us on **0845 140 1000**.

Keep your money safe by knowing where it is

There is no time limit for the presentation of cheques, however if you have issued a cheque which has not been presented by the payee within six months we recommend you place a stop on the cheque. There is a charge for this service. We also recommend you avoid holding excess stock of cheques and shred any obsolete stock.

Make fraud easier to detect by introducing procedures that are consistent

Whatever your method, whether you write your cheques or use a computer, make sure your procedure is consistent. When handwriting your cheque, ensure it is completed, signed and dispatched the same day. If you use a computer to overprint your cheques ensure the size and font is the same and, again, dispatch the cheques the same day.

Make it difficult for fraudsters to defraud your account by keeping your stationery under lock and key

Keep your money safe by ensuring all stationery is stored in a secure place - particularly overnight. Take care and check against the possibility of individual cheques being removed from the middle of your cheque book or from your computer cheque stock.

Don't pre-sign your cheques

Many customers elect two authorised

people to sign their cheques. Before signing the cheque it is important that each signatory checks supporting documentation to ensure the payment is valid. We therefore recommend that you never pre-sign cheques.

Receiving payment by cheque or banker's draft

Never accept a cheque or banker's draft from someone who is not known to you. Remember, a banker's draft is not safe from fraud, so other methods of payment are recommended especially when the payment is of high value. If you have been paid by banker's draft, before using the funds, you should wait until you are certain it has cleared and the money is yours. You can calculate this date by using the cheque checker tool, which tells you when the cheque will clear, on the Cheque and Credit Clearing Company website: **www.chequeandcredit.co.uk**.

Protect your account by separating office duties

Separate office duties to avoid conflict of interest or opportunities for abuse. We recommend you allocate at least two different people to reconcile your accounts. The same applies when you appoint an external auditor.

What would you do if you knew a fraud had been committed?

Ensure you have up-to-date fraud policies and procedures promoting an anti-fraud culture. Everyone within your organisation needs to know how to act if an external or internal fraud occurs. It is crucial your organisation has a process to detect and deter fraud, thus reducing the level of risk and the size of any losses.

¹ One-off Standing Order - Upon receipt of your request the process takes four working days however, some Building Societies and banks in Scotland may exceed this by one day.

² CHAPS - Receipt of your request by 2:30pm will guarantee same day payment.

³ Bill Payment - Once the payment is authorised, the beneficiary will receive the funds within three working days, however, Building Societies and banks in Scotland may exceed this by one day.

Make sure you have strong internal controls and efficient account reconciliation



A fraud can be committed with relative ease. To do this, an individual, whether within the organisation or outside the organisation, must first know that there are available funds for them to steal, and intend to commit the fraud. There may be a high chance the individual has the opportunity to commit fraud if sufficient controls are not in place to deter the individual.

In the case of safeguarding your stationery and to stop it getting into the wrong hands, make certain it is kept locked away both day and night. Treat your stationery as if

it were cash. When using a safety deposit box or safe, opt for dual-control access as this will provide you with extra control and prevent misuse.

We encourage you, wherever possible, to have more than one individual who is responsible for a specific job within your office. This will increase your ability to detect an internal problem.

If an individual has sole access, they have the ability to conceal irregularities which will prove more difficult for you to identify.

Case studies - Internal controls

Mr A contacted the Bank for an account balance and discovered it had reduced dramatically. An internal investigation identified that another signatory, Mrs B, had used pre-signed cheques for her personal use. It had not been discovered due to the lack of internal controls as Mrs B had prime responsibility for the account stationery and reconciliation.

When questioned by the Bank, Mr A admitted that he had trusted his co-signer enough to not ask for supporting documentation for any cheque either pre-signed or presented to him. This oversight led to a loss of £51,000.

...take care of your money - do not pre-sign your cheques.

Our advice to you

In order to avoid internal fraud, you should ensure that you have controls in place to minimise the risk of loss. The best way to do this is to have dual-control for the issuing and signing of cheques. Make sure that when a cheque is issued, you have a valid invoice to justify the payment and that a second person checks this before co-signing. Keep your cheque book locked away and **NEVER** pre-sign cheques. We recommend you carry out a regular audit of your cheque book and make sure all cheques are accounted for. By doing this, you will identify a problem almost

immediately and reduce any potential loss.

An alternative method of payment for suppliers or any such beneficiary is our Bill Payment service through Internet Banking. This will provide you with full dual-control over the frequency and amount of each payment.

To find out more on the different methods of payment available to your organisation, please contact the Banking Operations Team:

0845 140 1000

Case studies - Overseas transfers

Following receipt of an overseas transfer request, the Bank contacted the customer to ask if the request was legitimate as it wasn't on the Bank's Transfer of Funds Overseas form and one of the two signatures did not match the customer account mandate. Mr C advised the Bank that the request was fraudulent as he would never send funds abroad especially for such a high value (equivalent of £21,500).

The Bank questioned the possibility of the customer's bank details being available to the public. Mr C confirmed that their bank details are published on the internet

for Gift Aid purposes and the signatures of directors are shown on the annual accounts which is published on their website.

...fraudsters are taking advantage of attempts to make donating easy.

Our advice to you

Although it is reasonable to expect account information to be published on Gift Aid forms, where possible we recommend you open a 'deposit only' account for such donations. If you feel this isn't an option that suits you, you may wish to introduce an alternative method so the donor can email you to request a form. This way you can

monitor and track who you are sending your bank details to.

The Bank also appreciates the requirement to include the signature of the company director and secretary on the annual accounts and understands that you may have additional signatories on your account other than those mentioned; however it is good practice to publish an unsigned version on your website.

Don't be exposed to the risk of fraud by supplying your bank account details.

Checklist for assessing your risk to fraud

It's only too easy to think of fraud as someone else's problem. However, remember that all organisations are vulnerable to fraud of one sort or another.

To understand the potential consequences of fraud on your organisation and to establish an anti-fraud culture, we recommend you introduce the appropriate policies, controls and procedures to reduce your exposure to fraud.



Do you have a fraud policy statement to communicate your organisation's approach to fraud?

Such a statement may include some or all of the following:

- Allocation of responsibilities for the overall management of fraud;
- The procedures which staff should follow if fraud is discovered;
- Guidance on training for the prevention and detection of fraud;
- Reference to response plans that have been devised to deal with and minimise the damage caused by fraudulent attack.

Your fraud policy statement should be simple, focused and easy to understand.

Does your organisation have a fraud response plan?

It is important that managers know what to do in the event of fraud so that they can act without delay. An effective fraud response plan should reflect your organisation's circumstances and the likely nature and scale of losses. A fraud response plan should cover:

- To whom the fraud or suspicion of fraud should be reported in the first instance (e.g. senior managers, personnel or internal audit);
- How your organisation should investigate fraud;
- How to secure evidence in a legally admissible form;
- When and how to contact the police;
- How to initiate recovery action;
- Who else to contact for advice (e.g. insurers, regulatory bodies, legal advisers, parent department, press office);
- How to circulate the lessons learnt from fraud cases.

The guidelines are provided by the Fraud Advisory Panel. For more information, including advice on fraud policy statements and fraud response plans, visit www.fraudadvisorypanel.org.

To assist you, the following publications produced by the Cheque and Credit Clearing Company at: www.chequeandcredit.co.uk

- **Business Users of Cheques - Using Company Cheques Safely**
Best practice guidelines for organisations using the Bank's standard cheque stationery (users of company cheques).
- **Business Users of Cheques - Personalising Company Cheques**
Best practice guidelines for organisations wishing to personalise their own cheques including adding the MICR code line.
- **Business Users of Cheques - Using Laser Printers to Infill Company Cheques**
Best practice guidelines for organisations using or wishing to use computer printers to overprint their cheques.



If you have experienced a fraud within your organisation or have personally been a victim, please email us at fraud@unity.co.uk as we are interested in hearing how you dealt with it and what measures you have introduced since it happened. This information will benefit other customers who may need your guidance.

A summary of the Bank's advice to you

- ✓ Check your statements frequently and advise the Bank of any discrepancies by calling **0845 140 1000** or by emailing **fraud@unity.co.uk**.
- ✓ Consider other methods of payments for large value transactions, such as Standing Orders, CHAPS or Bill Payments.
- ✓ Never pre-sign blank cheques.
- ✓ If you issue a cheque which is not presented within six months, do not assume that it has become invalid - you should stop the cheque. You can stop a cheque for a fee of £10 per cheque by calling **0845 140 1000** or cheques can also be stopped using our Internet Banking Service for a reduced fee of £5.
- ✓ Whether you complete your cheque by hand or overprint by computer, make sure your procedure is consistent, so that any differences can be identified more easily and quickly.
- ✓ In order to deter fraudsters copying or removing cheques, you should dispatch cheques immediately and ensure they are taken to the post box or Post Office®, rather than have them dispatched via an internal postage collection service.
- ✓ Treat unused cheques as securely as you would treat cash by keeping your stationery locked away.
- ✓ Allocate responsibility to at least two people for issuing cheques and undertaking reconciliation of your bank accounts.
- ✓ If you are publishing a copy of your annual accounts on your website make sure it does not feature the signatures of any signatories to your accounts.
- ✓ If you supply a Gift Aid form on your website, you may wish to open a 'deposit only' account for such donations. Alternatively, ask the donor to request a Gift Aid form via email, giving you control over who you send your bank details to.
- ✓ Ensure your internal policies are up-to-date. It is important to know what to do in the event of a fraud so you can act without delay.

An effective and timely response is vital to minimise the impact of fraud to your organisation. Act now and identify any vulnerable areas within your organisation.

Disclaimer

Unity Trust Bank has provided you with the checklist as a guide which is not exhaustive. We have made every effort to make this checklist comprehensive; compliance with it does not guarantee that your organisation will not be a victim of fraud. Unity Trust Bank and the contributors to this information guide accept no responsibility for any action taken by parties as a result of reading it. Each organisation should take appropriate independent advice on the management of fraud risk.

t: 0845 140 1000 e: fraud@unity.co.uk w: www.unity.co.uk