

## Financial fraud is increasing at an alarming rate each year

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

**According to figures published by APACS (the Association for Payment Clearing Services) in 2003, the amount of attempted frauds totalled £556.4m. In 2004 £665m frauds were attempted. Any fraud which succeeds has a dramatic impact on the organisation that is targeted.**

Unity Trust Bank is working with customers in an attempt to prevent you becoming a victim of a serious fraud. 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.

### **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 Order<sup>1</sup> payments or Telegraphic Transfers<sup>2</sup>. Alternatively you may wish to use Internet Banking where payments can be sent to any bank account via the Bill Payment<sup>3</sup> service. This facility is available to accounts with dual authority.

Authorised and regulated by the Financial Services Authority.  
Registered in England and Wales, no 1713124. Registered office, Nine Brindleyplace, Birmingham B1 2HB

### **Keep your money safe by knowing where it is**

Place a stop on all cheques that have not been presented within six months no matter what the value.

### **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.

### **Do you pre-sign your cheques?**

Many customers elect two authorised people to sign their cheques. Before signing the cheque it is important that each signer checks supporting documentation to ensure the payment is valid.

### **Protect your account by segregating office duties**

Segregate office duties to avoid conflict of interest or opportunities for abuse. We recommend you allocate at least two different people to reconcile your accounts.

### **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.

**“You’re never too big or too small to be a target of fraud”**

**“We’re only a small charity with little funds; we’ll never be a target”**

**“It will never happen to us; well, we haven’t been stung yet!”**

1 One-off Standing Order - Upon receipt of your request the process takes four working days however, some Building Societies and Banks within the Scotland area may exceed this by one day. There is a charge for this service.  
2 Telegraphic Transfer - Receipt of your request by 14:30 will guarantee same day payment. There is a charge for this service.  
3 Bill Payment - Once the payment is authorised, the beneficiary will receive the funds within 3 working days, however, Building Societies and Banks within the Scotland area may exceed this by one day.

# ...fear of detection is far greater than

## Strong internal controls and efficient account reconciliation is imperative in any organisation

A fraud can be committed with relative ease. The individual, whether within the organisation or outside the organisation, must first have the knowledge that there are available funds to acquire, followed by the intent 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 safe guarding 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 utilising a safety deposit box or safe, opt for dual-control access as this will provide you with extra control and prevent easy admission.

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

If an individual has sole access, they have the ability to conceal irregularities.

### Case studies – Overseas transfers

Following receipt of an overseas transfer request, the Bank performed a 'call-back' procedure asking the customer to confirm the details of the request to ascertain its authenticity. At this stage Mr C alerted the Bank that the request must be fraudulent as they would never send funds abroad especially for such a high value (equivalent of £21,500).

The Bank questioned the possibility of their 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 on the Report and Accounts 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 Report and Accounts and understands that you may have additional signatories on your account other than those mentioned; however it is recommended that you place an unsigned version on your website.

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

### Case studies – Internal controls

Mr A became aware that funds had been misappropriated when he contacted the Bank for an account balance and noticed it had reduced dramatically. An internal investigation identified that his co-signer, 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.

**For further advice on your options, please contact the Customer Services Team:**

**0845 140 1000**

# an fear of committing the crime.

If you have experienced a fraud within your organisation or have personally been a victim, please email us at [fraud@unity.co.uk](mailto: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.

## To assist you, the following publications produced by APACS are available upon request:

Best Practice Guidelines for organisations using the Bank's standard cheque stationery (users of company cheques).

Best Practice Guidelines for organisations wishing to personalise their own cheques including adding the MICR code line.

Best Practice Guidelines for organisations using or wishing to use computer printers to overprint their cheques.

Please request your preferred copy by emailing us at [fraud@unity.co.uk](mailto:fraud@unity.co.uk)

## Best Practice Guidelines<sup>4</sup> Checklist for assessing your risk to fraud

It's only too easy to think of fraud as someone else's problem however, it must be remembered that all organisations are vulnerable to fraud of one sort or another.

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

### Does your organisation have a **Fraud Policy Statement** to communicate the organisation's approach to fraud?

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

- 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 easily understood.

### 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 be closely tailored to your organisation's circumstances and should reflect 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 disseminate the lessons learnt from fraud cases.

For further assistance you may wish to access [www.uk-fraud.info](http://www.uk-fraud.info) where the Association of Chief Police Officers (ACPO) has provided an example of a fraud policy statement which you may choose to adapt to suit your organisation. Alternatively you may find it useful to access [www.hm-treasury.gov.uk](http://www.hm-treasury.gov.uk) for guidance on a fraud response plan.

## Next Steps

### A summary of the Bank's advice to you

- Check your statements frequently and advise the Bank of any discrepancies
- Consider other methods of payments for large value transactions
- 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. Remember you can stop a cheque on the Internet for a reduced fee of £5
- Whether you complete your cheque by hand or infill by computer, ensure your approach is consistent
- 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 cash by keeping your stationery under lock and key!
- Allocate responsibility to at least two people for issuing cheques and undertaking reconciliation with bank statements
- If you are placing a copy of your Report and 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 your website, 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 the success of 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 construct this checklist; 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.

Source: The Home Office, Association of Chief Police Officers 'Fraud Prevention Report', APACS (UK payment association), The Fraud Advisory Panel and BBA (British Bankers Association).

**0845 140 1000** [www.unity.co.uk](http://www.unity.co.uk)

Registered in England and Wales, no 1713124. Registered office, Nine Brindleyplace, Birmingham B1 2HB

**Unity**  
TRUST BANK