Cheque Fraud Prevention

Introduction
Cheque fraud has become big business. Overseas and Australian trends point to escalating cheque fraud attempts and losses. It emerges as one of the significant challenges facing business and financial institutions today and there are clear warnings that no one is immune from cheque fraud.

Cheque fraud may be internal or external and may take many forms. Business and financial institutions must develop risk management strategies to deal with a host of possibilities. Apart from the risk of cheque theft, other risks include payment on fabricated supplier invoices, forged signatures, alterations to the payee name and amount and duplicated or counterfeit cheques.

The purpose of this brochure is to provide your business with specific tips on how to improve your internal controls to reduce the potential for cheque fraud.

Business owners and financial controllers should carefully consider how these tips may apply to your business, and whether other measures to reduce the potential for cheque fraud may also be appropriate. Refer to your accountant for measures that may suit your particular business.

Issuing and Reconciling cheques

Preparation
- Cheques must be completed in a way that deters fraudulent alteration. Ensure that a strong, bold and consistent font is used and that no gaps are left in the completion of the payee name, amount in words and amount in figures.
- Printing systems should be of a sufficient quality and maintained to ensure cheque details are clear and legible.
- If completed in ink, use indelible ballpoint or permanent ink (preferably black).

Signing of cheques
- Never sign cheques in blank – ensure that cheques are signed only after all details have been completed.
- Cheques with preprinted signatures must be more closely controlled and regularly audited.
- Limit the number of authorised signatories and regularly audit your business signing authority registered at the bank.
- A ‘Two to Sign’ authority may be warranted in some circumstances although this is no substitute for proper office controls.
- Ensure your Annual Report and any other public documents, including those displayed on your business website, do not display signatures of your authorised cheque signatories.

Reconciliation of your account
- Reconcile your cheque account promptly and regularly (suggested daily usage of National Online or National Internet Banking) with independent overview by the appropriate level of management. Quick fraud detection increases the likelihood of loss prevention and/or recovery.
- Separate the cheque writing and account reconciliation functions. This provides greater safeguard against an employee writing fraudulent cheques and covering it up. The reconciler will be in a position to detect the crime, unless the employees are acting in collusion.
- Independently confirm any spoiled and non-presented cheques – less than honest office staff may use these to their own advantage.
- Consider opening a separate account specifically for higher value cheques so that large disbursements can be easily monitored. You may elect to use a separate signing authority on such an account.

Ordering and Maintaining Cheque Stocks:
- Ensure a thorough (and unannounced) cheque stock reconciliation is performed on a regular basis.
- If cheques are lost, stolen or misplaced request your bank to record a ‘Stop Payment’.
- If your business is one which purchases Specially Printed Forms (ie you do not use the standard cheques supplied by your bank) you should be sure to use an Australian
Take prompt action on overdue accounts and missing cheques. If a cheque payable to you is stolen, ask the sender to stop payment and issue a replacement. Advise details of stolen cheques to the Police.

Outgoing mail
- Avoid sending high value cheques via standard mail services to reduce the possibility of interception of cheques by fraudsters.
- Consider introducing a policy where the use of electronic and direct payment options is mandatory for invoices over prescribed amounts.
- Avoid using preprinted company envelopes that may draw attention to the contents.
- Avoid using window-faced envelopes, and where they are used ensure that cheques are concealed within other correspondence.
- Maintain a list of creditors and/or areas where cheques have previously been stolen and use alternative delivery processes, i.e. electronic and direct payments, courier, certified or registered mail.

For more information on appropriate fraud prevention measures for your business, we suggest you contact your accountant. For more information on the National’s business account and payments products, please contact your National banker.

Internal security
- Secure all bulk supplies of cheques in a locked facility under dual custody and limit the number of people authorised to access and handle your cheques. Use a bulk cheque register to record the transfer of smaller ‘working’ supplies to authorised staff.
- Ensure ‘working’ supplies are secured in a locked facility after working hours.
- Larger firms should maintain a record of those employees who work on each print batch.
- Develop and reinforce a series of best practices for the office, such as ‘Never leave blank or incomplete cheques unattended’.
- Your reconciliation procedures should ensure spoilt, obsolete or damaged stock is destroyed immediately in terms of your reconciliation procedures, and duly noted in the bulk cheques register.
- Restrict access to cheque printing areas.

Supplying banking details
Watch out for telephone, facsimile or email requests for your banking details. This information may fall into the hands of fraudsters who will attempt to use this information to fraudulently obtain funds. Your Accounts Receivable area should validate any such requests.

Employee recruitment policies
- Make sure you know who you are hiring to handle your money! Diligent reference and background investigations (police checks) on all prospective employees are important so you know that you are not hiring someone with a past record of financial abuse.
- Verify claimed references and educational qualifications.
- Conduct random audits and enforce annual leave policies. Many instances of internal fraud are detected when an offender is on leave. Offenders often resist taking leave.

Mail fraud mitigation strategies
Inward mail
- Have inward mail sent to a secure mail address/box to reduce the risk of interception.
- Mail should be opened by two people and cheques received should be recorded without delay.

Other Key Points
- Ensure that you assign separate Accounts Payable functions to more than one person making each person responsible for different steps in the process. This division of responsibility (known as segregation of duties) makes it more difficult for individual employees to tamper with cheques and payments.
- Many frauds have been committed by employees who falsify invoices for payment. A robust process of checking and verification should exist which ensures that no cheque is drawn, signed and issued except where a responsible officer has confirmed the authenticity and validity of the underlying invoice, and has duly authorised payment of the account.

Maintain adequate physical security for your cheques
External Security
- Ensure premises have appropriate external security measures such as alarms, security staff, fencing and lighting.
- Consider changing all locks on your premises periodically.

Internal security
- Secure all bulk supplies of cheques in a locked facility under dual custody and limit the number of people authorised to access and handle your cheques. Use a bulk cheque register to record the transfer of smaller ‘working’ supplies to authorised staff.
- Ensure ‘working’ supplies are secured in a locked facility after working hours.
- Larger firms should maintain a record of those employees who work on each print batch.
- Develop and reinforce a series of best practices for the office, such as ‘Never leave blank or incomplete cheques unattended’.
- Your reconciliation procedures should ensure spoilt, obsolete or damaged stock is destroyed immediately in terms of your reconciliation procedures, and duly noted in the bulk cheques register.
- Restrict access to cheque printing areas.

Supplying banking details
Watch out for telephone, facsimile or email requests for your banking details. This information may fall into the hands of fraudsters who will attempt to use this information to fraudulently obtain funds. Your Accounts Receivable area should validate any such requests.

Employee recruitment policies
- Make sure you know who you are hiring to handle your money! Diligent reference and background investigations (police checks) on all prospective employees are important so you know that you are not hiring someone with a past record of financial abuse.
- Verify claimed references and educational qualifications.
- Conduct random audits and enforce annual leave policies. Many instances of internal fraud are detected when an offender is on leave. Offenders often resist taking leave.

Mail fraud mitigation strategies
Inward mail
- Have inward mail sent to a secure mail address/box to reduce the risk of interception.
- Mail should be opened by two people and cheques received should be recorded without delay.

Other Key Points
- Ensure that you assign separate Accounts Payable functions to more than one person making each person responsible for different steps in the process. This division of responsibility (known as segregation of duties) makes it more difficult for individual employees to tamper with cheques and payments.
- Many frauds have been committed by employees who falsify invoices for payment. A robust process of checking and verification should exist which ensures that no cheque is drawn, signed and issued except where a responsible officer has confirmed the authenticity and validity of the underlying invoice, and has duly authorised payment of the account.

Maintain adequate physical security for your cheques
External Security
- Ensure premises have appropriate external security measures such as alarms, security staff, fencing and lighting.
- Consider changing all locks on your premises periodically.

Internal security
- Secure all bulk supplies of cheques in a locked facility under dual custody and limit the number of people authorised to access and handle your cheques. Use a bulk cheque register to record the transfer of smaller ‘working’ supplies to authorised staff.
- Ensure ‘working’ supplies are secured in a locked facility after working hours.
- Larger firms should maintain a record of those employees who work on each print batch.
- Develop and reinforce a series of best practices for the office, such as ‘Never leave blank or incomplete cheques unattended’.
- Your reconciliation procedures should ensure spoilt, obsolete or damaged stock is destroyed immediately in terms of your reconciliation procedures, and duly noted in the bulk cheques register.
- Restrict access to cheque printing areas.

Supplying banking details
Watch out for telephone, facsimile or email requests for your banking details. This information may fall into the hands of fraudsters who will attempt to use this information to fraudulently obtain funds. Your Accounts Receivable area should validate any such requests.

Employee recruitment policies
- Make sure you know who you are hiring to handle your money! Diligent reference and background investigations (police checks) on all prospective employees are important so you know that you are not hiring someone with a past record of financial abuse.
- Verify claimed references and educational qualifications.
- Conduct random audits and enforce annual leave policies. Many instances of internal fraud are detected when an offender is on leave. Offenders often resist taking leave.

Mail fraud mitigation strategies
Inward mail
- Have inward mail sent to a secure mail address/box to reduce the risk of interception.
- Mail should be opened by two people and cheques received should be recorded without delay.

Other Key Points
- Ensure that you assign separate Accounts Payable functions to more than one person making each person responsible for different steps in the process. This division of responsibility (known as segregation of duties) makes it more difficult for individual employees to tamper with cheques and payments.
- Many frauds have been committed by employees who falsify invoices for payment. A robust process of checking and verification should exist which ensures that no cheque is drawn, signed and issued except where a responsible officer has confirmed the authenticity and validity of the underlying invoice, and has duly authorised payment of the account.

Maintain adequate physical security for your cheques
External Security
- Ensure premises have appropriate external security measures such as alarms, security staff, fencing and lighting.
- Consider changing all locks on your premises periodically.

Internal security
- Secure all bulk supplies of cheques in a locked facility under dual custody and limit the number of people authorised to access and handle your cheques. Use a bulk cheque register to record the transfer of smaller ‘working’ supplies to authorised staff.
- Ensure ‘working’ supplies are secured in a locked facility after working hours.
- Larger firms should maintain a record of those employees who work on each print batch.
- Develop and reinforce a series of best practices for the office, such as ‘Never leave blank or incomplete cheques unattended’.
- Your reconciliation procedures should ensure spoilt, obsolete or damaged stock is destroyed immediately in terms of your reconciliation procedures, and duly noted in the bulk cheques register.
- Restrict access to cheque printing areas.

Supplying banking details
Watch out for telephone, facsimile or email requests for your banking details. This information may fall into the hands of fraudsters who will attempt to use this information to fraudulently obtain funds. Your Accounts Receivable area should validate any such requests.

Employee recruitment policies
- Make sure you know who you are hiring to handle your money! Diligent reference and background investigations (police checks) on all prospective employees are important so you know that you are not hiring someone with a past record of financial abuse.
- Verify claimed references and educational qualifications.
- Conduct random audits and enforce annual leave policies. Many instances of internal fraud are detected when an offender is on leave. Offenders often resist taking leave.

Mail fraud mitigation strategies
Inward mail
- Have inward mail sent to a secure mail address/box to reduce the risk of interception.
- Mail should be opened by two people and cheques received should be recorded without delay.

Other Key Points
- Ensure that you assign separate Accounts Payable functions to more than one person making each person responsible for different steps in the process. This division of responsibility (known as segregation of duties) makes it more difficult for individual employees to tamper with cheques and payments.
- Many frauds have been committed by employees who falsify invoices for payment. A robust process of checking and verification should exist which ensures that no cheque is drawn, signed and issued except where a responsible officer has confirmed the authenticity and validity of the underlying invoice, and has duly authorised payment of the account.