Fraud awareness & Information pack for ANZ Customers

INTRODUCTION

IS FRAUD THE SILENT PARTNER IN YOUR BUSINESS?

If fraud was a country it would rate as the fifth largest economy in the world - according to the KPMG fraud barometer. Of greater concern is that 80% of frauds committed on a business were committed by their own staff. More often than not these crimes are committed by opportunistic staff who exploit weak controls.

The purpose of this pack is to raise your awareness and provide you with some useful tips on how to improve your internal controls and reduce the potential for fraud losses.

As a business owner or financial controller you should carefully consider how these tips might apply to your business, and whether other measures to reduce the potential for fraud might also be appropriate.

Areas covered in this pack will include;

- Cheque fraud
- Invoice fraud
- Scams
- Identity theft
- Card skimming fraud
- Email hijacking
- Access controls
- Financial governance
- Employee policies

CHEQUE FRAUD

Cheque fraud is still one of the main challenges facing business and financial institutions today. It can be perpetrated by those inside a business as well as by external parties and can take a number of forms, including;

- Materially altered (includes payee and values).
- Forged (signatures).
- Duplicate or counterfeit cheques.
- Kiting (circulating valueless cheques between accounts to draw on uncleared funds).

IMPORTANT CONSIDERATIONS TO AVOID CHEQUE FRAUD INCLUDE:

- Never pre sign blank cheques.
- Ensure that cheques are signed only after all details have been completed.
- Cheques must be prepared for issue in a way that deters fraudulent alteration, such as by using complete payee details.
- Try to make sure a strong, bold and consistent font is used and that no excessive spaces remain between words or between numbers, with words and numbers filled in from the left-hand side.
- Limit the number of authorised signatories.
- Regularly audit your business' signing authority – at least every 12 months.
- Avoid single signature authorities and implement a minimum of two to sign.
- Maintain a cheque register to record the serial number range of cheque stocks received.
- If cheques are lost, stolen or misplaced immediately inform your financial institution and request a 'Stop Payment' and/or cancellation of cheques.
- If you are printing your own cheques or having them printed ensure security features are included to deter counterfeiting and fraudulent alteration.
- Reconcile cheques to statements.
- Secure cheques and limit access to cheque stocks/books.

INVOICE FRAUD

Invoice Fraud is becoming more and more prevalent and, although it can be perpetrated in a number of different ways, it can be summarised as occurring when a genuine invoice is intercepted or issued by fraudsters who change the details on the invoice to an account they control. Quite often, the only way a business discovers they are a victim of Invoice Fraud is when the genuine supplier contacts them regarding non-payment.

WAYS IN WHICH INVOICE FRAUD CAN OCCUR

- The Business is contacted by a fraudster, either by phone, email or fax purporting to be their supplier and falsely informs the Business that their account details have changed.
- The Business' IT systems may be hacked or become infected by Malware. The account details of the supplier are changed in the internet banking environment and the next time the Business attempts to pay the supplier, they are inadvertently transferring money directly to the fraudster.
- The Business' mail has been intercepted and adjustments have been made to the account details on the invoice. Or the invoice is replaced with a fraudulent substitute.

DETECTING INVOICE FRAUD

Invoice Fraud relies upon the interception and alteration of payments so therefore the best place to detect Invoice Fraud is at these points of compromise.

- Check the physical invoices received from suppliers and compare it to an invoice you know to be genuine. Altered/fraudulent invoices may utilise different ink, fonts or the company logo may be different or blurred. Contact details such as phone numbers and email addresses may have also changed.
- In the case of changed email addresses, an altered address may look almost identical, but for a subtle change to the domain (i.e. *".org"* now reads *".com").*

TIPS FOR REDUCING THE RISK OF INVOICE FRAUD

- Keep your anti-virus programs up-to-date to ensure your Business computers are not susceptible to Malware.
- Always confirm changes to bank details with the supplier requesting the change. Always use the contact details for the supplier that you have on file, rather than relying on those provided in correspondence requesting the change.
- Train your staff to look out for irregularities on invoices, particularly relating to changes in details and appearance.
- Consider sending a confirmation correspondence notifying your supplier once payment has been made, confirming the details of the payment.
- Contact suppliers prior to making payments using new or amended details.

SCAMS

Scams remain one of the most simple, yet effective ways people fall victim to fraud. Although scams can come in a variety of different forms, they generally present victims with a scenario that is 'too good to be true'. Victims will either be receiving funds for very little output (and these funds could be proceeds of crime) or parting with funds for a reward.

WARNING SIGNS THAT YOU, OR YOUR CUSTOMERS, ARE THE TARGET OF A SCAM

- Have you won a lottery you never entered?
- Have you met someone online, who is requesting you send money to them for

investment or for a personal tragedy (they are in danger, or a relative has become sick)? You may have also been asked to receive money under these circumstances.

- Have you been invited to participate in an investment scheme that offers exceptionally high returns for relatively low risk?
- Are you receiving commission for accepting funds through your Bank or PayPal?
- Are you cashing or depositing cheques as part of a Work-From-Home program?
- Have you purchased something online which has never arrived?
- Have you responded to an email asking you to confirm, update or provide your banking information?
- Have you been asked to pay money to receive an inheritance for a relative you did not know?
- Have you been overcharged fees and are asked to pay a nominal amount to have the fees reimbursed?
- Have you been asked to transfer money overseas using Western Union, Money Gram or another Money Service Business (MSB)?

If you have answered yes to any of the questions above, you should contact an ANZ representative immediately.

AVAILABLE REFERENCE MATERIAL

- anz.com
- Scamwatch.govt.au

IDENTITY THEFT

Identity theft is a type of fraud where someone gains a financial benefit by pretending to be someone else. In order to take over your identity, the fraudster needs to obtain your personal information, which they can steal from you using a variety of methods. Fraudsters may use your identity to obtain credit, access your funds and even to open bank accounts.

EXAMPLES OF HOW FRAUDSTERS CAN GAIN YOUR PERSONAL INFORMATION INCLUDE

- Intercepting your mail.
- Going through your bins to obtain documents which have not been complete destroyed.
- Through "Phishing"[1] scams, such as an email or text message that asks for your personal or banking details. Phishing emails often look like they have originated from legitimate sources, such as your Financial Institution.

TIPS TO HELP PREVENT IDENTITY THEFT

- Secure your personal documents at home and work.
- Ensure you destroy documents when disposing of them.
- Secure your mailbox with a lock, and ensure you update your address with all organisations when you move.
- Ensure you have strong passwords and up to date anti-virus software installed on your computer.
- Do not provide any personal or banking information via email.
- Do not input personal or banking information into a website unless you are certain it is genuine. Log directly onto websites by typing the link in the address bar, do not click on any links in emails.
- Ensure you check your bank statements regularly, and contact your bank if you do not recognise any of the transactions.

CARD SKIMMING FRAUD

[1] A Phishing email has the appearance of deriving from an authorised source and fraudulently requests confidential information

Card skimming fraud occurs when a fraudster illegally collects data from the magnetic strip of a credit or debit card. The fraudster then uses this card information to make fraudulent transactions.

WAYS IN WHICH CARD SKIMMING CAN OCCUR

- A skimming device may be placed over a legitimate ATM to copy the card data when the card is used at an ATM.
- Cards that offer a contactless payment method (such as "Paywave" or "Touch and Go") can have their details obtained by fraudsters who have a portable card reader. The portable card reader needs to be within a certain distance of the card it is attempting to read.
- Legitimate Point of Sale (POS) terminals (such as EFTPOS) can be replaced with fake terminals that capture card data and/or PIN.

TIPS FOR REDUCING THE RISK OF CARD SKIMMING FRAUD

- Be vigilant with any ATM which looks unusual. Report anything unusual immediately to the Bank, do not attempt to remove the device.
- Conceal your PIN when using an ATM.
- Consider storing your card in a safe container which is impenetrable by a portable card reader (such as foil lined wallets).
- Treat your card like cash and never lose sight of it. If possible, avoid giving it to a shop assistant or waiter and letting them walk out of your sight.
- Check your bank statements regularly to ensure you recognise all of the transactions. If there are any that you do not recognise, contact ANZ immediately.

EMAIL HIJACKING

Email Hijacking occurs when fraudsters gain unauthorised access to a personal or business email account and then send emails from that account to Financial Institutions seeking to conduct urgent transactions. It can be thought of as a type of electronic identity takeover.

EMAIL HIJACKING MAY OCCUR AS FOLLOWS

- A personal/business email account may have been compromised through hacking or via a Phishing email.
- An email may then be sent to the Financial Institution by the fraudster, purporting to be the customer, requesting an account balance or a Telegraphic Transfer (TT).
- In an attempt to avoid the Financial Institution's call-back verification process, the fraudster will indicate that they are stuck in a business meeting, or on their way to a funeral, and as a result are unable to answer any phone calls.

HOW TO AVOID EMAIL HIJACKING

- Keep your email account secure: Never provide your email address and password to anyone.
- Change your passwords immediately if you suspect they have been compromised.
- Change your password regularly and use strong passwords which are hard to guess.
- From a business perspective, always implement call-back verification processes to customers or suppliers who make transaction requests over email.
- It is important to have updated anti-virus software and strong passwords to help minimise the risk of hacking.

HOW TO DETECT EMAIL HIJACKING

If one of your customers or suppliers has fallen victim to email hijacking, you may receive an urgent request for a Telegraphic Transfer. You may also notice;

- A change in the way the customer usually corresponds (i.e. poor spelling and grammar).
- A refusal to confirm the request by phone.

GENERAL PREVENTATIVE INITIATIVES

ACCESS CONTROL

Staff members who have exploited access control weaknesses are often reported in cases of internal fraud. Therefore, adequate controls such as restricting systems access to staff on a needs only basis and limiting access to sensitive documents is an important fraud prevention initiative.

Some basic steps to enhance access control in your business include

- Enforce a policy where all confidential documents, cheques and bank statements are locked away when not in use.
- Provide information and documents on a "need to know" basis.
- Restrict access to banking information, payment instruments (such as cheques) and payment systems (such as internet banking). Regularly review staff access to this information, and remove anyone who no longer requires access.
- When a staff member leaves your business, ensure all equipment (e.g. laptop, phone etc.) is returned, and staff access to the building and all systems is immediately revoked.
- Change any passwords to payment systems to which they may have had access.
- Encourage staff to change their passwords regularly.

FINANCIAL GOVERNANCE

Practicing good financial governance may help prevent fraud in your business. In its simplest meaning, financial governance refers to a system of checks and balances to make sure processes run correctly.

Considerations

- Conduct regular audits on financial accounts and inventory stock.
- Regularly reconcile your financial accounts.
- Consider conducting surprise cash counts for businesses who are involved in cash handling.
- Make sure your business separates duties, for example the same staff member cannot raise an invoice and also approve the payment.

EMPLOYEE POLICIES

Employees can be your best asset or your greatest liability if they are provided with the opportunity to commit fraud.

Considerations

- Develop a Code of Conduct that sets minimum standards of conduct and behaviour for all employees and contractors.
- Have a clear policy on allowance expense claims.
- Develop effective employment screening processes including proper reference checks, police checks and qualifications.
- Enforce a minimum leave policy – many instances of internal fraud are detected when the employee committing the fraud is on leave; so be alert to those who are resistant to taking leave.
- Be alert for unusual spending patterns or changed employee behaviour; new cars, expensive clothes, holidays etc.
- Encourage your employees to raise any concerns they may have observed in regards to other employees possible

dishonest actions that could impact on your company.

- Ensure senior management is committed to controlling the risk of fraud and corruption.
- Demonstrate a policy of referring all internal fraud matters to police for prosecution regardless of financial impact.

FRAUD CONTROL PLANS

ANZ strongly encourages you to implement an effective fraud control plan - you know your business better than anyone else and you will be able to identify your key fraud risks. This makes good business sense and will also help you to avoid potential fraud losses.

FOR FURTHER INFORMATION

For ANZ employees, search for "Group Investigations" on Max to find your local contact.

FRAUD CONTROL CHECKLIST

PLANNING AND RESOURCING

	✓
Do you have a formal documented fraud policy that has been communicated to all staff?	
Are the fraud policies/processes and avenues to escalate concerns well documented and understood?	
Has a detailed assessment of fraud risks been undertaken?	
Have risks identified been documented in a risk register or control plan?	
Has a plan been implemented to review the fraud risks periodically?	
If risks have been identified, have you estimated a potential cost if the risks eventuated?	
Have you identified a maximum risk appetite or tolerance for the risks identified?	
Have you got a resource that has responsibility for fraud risk management; such as a "Fraud Champion" or "Fraud Delegate"?	

PREVENTION

	✓
Has a culture been created where ethical behaviour is promoted and encouraged?	
Are all staff aware of internal fraud reporting processes and their individual responsibilities?	
Is staff system access regularly reviewed to ensure it is limited to the functionality required to fulfil their job function?	
Are passwords and access levels to key payment and banking systems regularly reviewed and changed periodically?	
Are key processes and functions regularly reviewed to ensure there is adequate segregation of duties?	
Are physical access records, like building access logs, periodically reviewed to ensure that staff are accessing building premises at "normal" and reasonable times?	
Have processes been implemented to secure negotiable instruments and assets (i.e. cheques books, merchant facilities, cash, taxi vouchers, physical assets like computers and/or equipment)?	
Does the business perform physical stocktakes of assets periodically? (e.g. laptops, tool of trade phones, Blackberries etc.)	

PREVENTION

	✓
Does the business monitor staff with excessive annual leave? Are policies in place to enforce minimum annual leave absences?	
Does the business monitor and validate the results of high performing staff in situations where incentive schemes are in place?	
Does the business implement a pre-employment screening process (i.e. previous employment, criminal record checks, and comprehensive reference checks)?	
Have steps been taken to independently review new and existing suppliers and customers?	
Have all new staff completed fraud awareness training?	

DETECTION

	✓
Is there a channel for staff to report suspicions of fraud anonymously?	
Is there a process in place to enable the prompt investigation of concerns?	
Is a consistent approach applied to staff who have engaged in fraud? For example, are staff aware that all fraud matters, regardless of value, are reported to the police for prosecution	
Are surprise audits (cash/inventory reconciliation) conducted in addition to regular checks?	
Are any software solutions implemented to detect fraud?	

RESPONSE

	✓
If fraud is detected, does the business have adequate procedures and resources to deal with the suspected fraud?	
Are protocols articulated for reporting confirmed fraud to the appropriate authorities?	
Does the business have a process through which stolen property or funds can be recovered?	
Is your business adequately insured against the risk of loss arising from fraud?	
Does the business regularly review and track their fraud losses to learn and assess if there are any control gaps that need to be addressed?	
Are major loss events reviewed to ensure process/product breakdowns are addressed and appropriately mitigated?	
Are fraud losses routinely reported to senior leadership?	

RESPONSE ✓

Are external fraud trends and losses being tracked to ensure emerging threats are being appropriately managed?	
Does the business report instances of fraud, bribery & corruption, including attempts and near misses, in an accurate and timely manner to senior company executives, regulators and company boards as required?	
Have new products and/or channels been reviewed by fraud experts prior to, and post deployment, to ensure that key fraud risks are being mitigated?	