Fraud

Fraud

Fraud is described as intentional deception and dishonesty through the use of false means or information – resulting in personal or financial gain.

A retail business can be defrauded in many ways, whether through your employees, your customers, other businesses and/or your suppliers. The most common types of frauds against retailers are:

- credit card fraud
- refund fraud
- supplier fraud
- card skimming
- counterfeit notes
- cheque fraud.

Credit cards

With the introduction of chip technology and the increased use of PIN numbers rather than signatures the risks to retailers has declined over recent years. Customers may still choose to sign rather than use a PIN. If customers use a signature make sure this is always checked.

Be alert for customers that display the following behaviours:

- try to rush through a sale or distract staff during the sale
- make purchases without regard to size, quality or price
- have no identification
- request transactions to be manually entered
- sign their name slowly or unnaturally.

To minimise the risk of credit card fraud, ensure staff always check the front and back of the card:

- check if the card is damaged
- check the expiry date
- check the printing and embossing – does it appear to have been changed?

- check the hologram is 3D and changes colour when it is tilted
- check that the card has been signed, and that the signature panel has not been altered
- ensure the customer's signature matches the signature on the card.

Other advice includes:

- Counterfeit cards are near indistinguishable to authentic credit cards. At times the magnetic stripe data may not match the bank details on the front of the credit card, that is the stripe data is for a different financial institution. MasterCard, Visa and AMEX cards have Ultra Violent/UV (black light) watermarks printed on the front of the card. MasterCard has the letters MC. Visa has a V across the 'Visa' word logo, while AMEX has that lettering across its card. A card that lacks these features under a UV light is fraudulent.

Following the above checks, if you are suspicious of the card, request further photo identification such as a driver's licence or passport.

Refund fraud

The legal right to obtain a refund requires that the customer has a valid receipt and that the product is either faulty or not suitable for the purpose for which it was sold. Many retailers however provide refunds to customers who have simply changed their mind. This is done as a form of customer service. However dishonest people will take advantage of this generosity by claiming refunds under fraudulent circumstances. Types of refund fraud include:

- customers who purchase goods at another store and return it to your store
- employees keeping receipts and using them to obtain refunds either for themselves or friends
- customers buy products at sale prices then return them for refunds at higher prices
- customers returning used products for refunds at full prices.

Consider the below tips to prevent refund fraud:

- only accept refunds with a valid receipt
- ensure all refunds for staff are processed by management
- ensure all returned goods are closely inspected
- implement a store policy around a specific timeframe that goods can be returned, e.g. 14 days.

Supplier fraud

Dishonest delivery people and suppliers can steal from you by delivering fewer goods to your store than you have been charged for on the invoice.

The simplest method of deterring this type of behaviour is by checking all deliveries to ensure that you are receiving what you have been charged for. Also consider the following suggestions:

- only allow one delivery to be processed at a time
- do not allow delivery people to enter your storeroom area or unload your delivery.

Fraud

Card skimming

Card skimming is a crime that is increasing globally. Sophisticated techniques are used by criminals to steal or skim data from a customer's card as it is swiped through a terminal. A customer's PIN may also be at risk of being stolen through these techniques.

For retailers, some criminals will steal EFTPOS terminals, make the required changes, and replace it. Other criminals may simply replace your terminal with one that has already been modified. In both instances, your terminal is targeted and accessed.

Some common ways your terminal can be modified are:

- someone posing as a technician has come to service your terminal
- distractions or disturbances are caused to remove attention from terminal
- terminals that have been left unattended or not secured down may be targeted.

Always ensure that you verify all service visits

Below are a few tips to reduce the likelihood of card skimming at your store. Ensure your terminal:

- looks the same and has no damage or modifications
- has the same number and types of cables
- has the correct serial number
- prints receipts indicating the right business name and address
- is clear of any hidden cameras
- is kept out of sight and reach of customers and lock them away whenever possible.

If you or your staff notice any modifications or changes to your terminals, missing terminals, or a suspicious technician servicing or replacing your terminal contact police immediately.

Counterfeit notes[1]

There are a few signs retailers can use to identify counterfeit money.

- Feel the note. Australian money is made using a special plastic polymer that is difficult to tear.
- Hold the note to the light and look for the Australian Coat of Arms when looking at the front of the note.
- The main design of the note is slightly raised printing and can be felt.
- Look for the seven pointed star inside a circle.
- Look for any distortion or undefined patterns in the background printing.
- Check that the note has a clear window and that it has a clear printed image: $5 note has a gum flower; $10 has a windmill; $20 has a compass; $50 has the Southern Cross and the $100 has a lyrebird. Also, in the window of the $10 note a wave pattern is slightly visible, and the numbers 20, 50 and 100 appear in the window of respective notes.

[1] Bizsafe (February 2006). Fraud and Business Scams.

Fraud

If you suspect that you have received a counterfeit note:

- advise the customer that you think that the note is counterfeit and that you are going to call the Police
- handle the note as little as possible and place it in an envelope or other protective covering
- notify the Police straight away.

For further information visit The Reserve Bank of Australia's guide to detecting counterfeit currency www.rba.gov.au/banknotes/counterfeit/detection.html

Cheque fraud

The use of cheques is generally declining and with it the risk to retailers. Perhaps the best way of reducing the risk of cheque fraud is by deciding not to accept cheques at all. If however you decide to accept cheques as payment for goods make sure that you do the following:

- Cheques may be entirely fraudulent. Look for spelling mistakes such as 'check' rather than 'cheque' and the quality of the paper.
- Ask for a suitable ID, Driver's Licence or Passport, record the details on the back of the cheque.
- Ensure that the cheque is signed in your presence and that the signature matches that on the ID.
- There are services available that are able to provide on the spot clearance of cheques. Your business should consider using this service.

Invoicing fraud

- Companies may be the victim of fraudulent invoicing by offenders sending fake invoices for goods or services. Be suspicious of invoices not correctly addressed or referenced. Identify the recipient in the company of the goods or service to ensure it was received for the amount specified. Offenders may register fake email addresses and websites for legitimate suppliers using a .com or other domain extension rather than a .com.au to advertise and receive inquiries, or use slightly different/similar spelling, therefore contact the supplier using details in the phone book to verify the authenticity of the invoice.