

Electronic fraud

In cases of electronic fraud involving unauthorised credit card transactions, the merchant bears the risk, not the financial institution or the legitimate owner of the credit card.

In light of this, it is important to be vigilant when processing sales, particularly over the telephone, by mail order or via the Internet.

Shane Ringin, general manager of Pro Active Strategies, recommends that in such a transaction it is essential that staff members obtain a credit card number, its expiry date and the full name, address and a contact telephone number for the cardholder.

'Having obtained this information, staff should always obtain an authorisation for all transactions in which a card is not presented, regardless of the value,' he said.

'Obtaining an authorisation for a card confirms that the card is valid and has not been reported lost or stolen and sufficient funds are available to cover the amount of the transaction being processed.'

'A short time after accepting the order, always call the telephone number provided to confirm details of the order. Record the time and date that the customer was spoken to and record it on the order.

'If the customer arranges to collect the goods from the store as opposed to having them delivered, ensure a credit card is presented and card imprint and signature obtained.

'Deliveries should be through a courier utilised and arranged by the client, not the customer. It is imperative that the delivery driver is instructed to deliver the goods to a person who is inside the premises, and obtains a signature. Drivers should be cautioned about delivering to hotels, motels or Post Office boxes, and wary of people who approach them outside delivery addresses to take possession of the goods.'

Unfortunately, according to Shane, there is little identification that can be obtained electronically that can be verified by businesses.

'The best case scenario would involve customers registering at the business prior to conducting online or phone transactions. Where this cannot be done, follow the procedure outlined earlier.'

Businesses can minimise the chance of being the victim of electronic crime by following these tips from Shane:

- Electronic terminals should never be left unattended where criminals can access them and compromise them by placing storage chips inside, or utilise them for refunds.
- All merchant equipment should be secured when not in use, including paper sales and credit vouchers.
- All Point of Sale terminals with refund capabilities should have a unique password to prevent unauthorised use.
- Businesses should watch for:
 - Large, one-off purchases that allow criminals to minimise the possibility of identification.
 - Larger than normal orders that maximise the use of stolen or counterfeit credit cards.
 - Multiple orders for the same item or big-ticket items.
 - Rushed orders or requests for overnight delivery to allow quick resale before fraud is detected.
 - Any orders shipped internationally to a customer or country not usually dealt with by the business.