CREDIT CARD FRAUD PREVENTION

NFRN
Federation of Independent Retailers

Credit card fraud is growing within retail premises and retailers must develop internal preventative procedures to ensure their account does not suffer losses, due to banks putting responsibility onto retailers. Retailers across the UK have had partial or permanent money withheld from their account due to their bank's dissatisfaction with the multiple transaction history within the store by the same customer over a short time period eg 2 days, 300 contactless transactions. The cases we have followed may have shown a tell-tale sign that retailers should have been alerted to fraudulent activity BUT given there is little guidance available to help retailers, the NFRN has developed a basic preventative guidance on what to look out for during the course of transactions with customers.

(Please note, this information is by no means infallible and is merely a guide to help prevent fraud within your business).

How to spot a counterfeit card

MasterCard and Visa issued cards have a number of identifying features that most counterfeit cards aren't able to copy:

- **First four digits of the embossed card number should also be printed directly below the main numbers. Check to make sure these match.**
- **Hologram – when the card is moved at the right angle, a brand image should become visible Visa has a dove and MasterCard has a globe.**
- **Ultraviolet motifs – if you have a UV detector, you can check the card's motif. If no image appears, the card may be a fake.**

Reasonable Activity of Contactless Transaction Per Customer

- As a Merchant you cannot turn off the Contactless facility, but you can refuse to accept contactless transactions – however this could be counter-productive as it will inconvenience your customers that require choice.
- Repetitive and multiple purchases of the same item through contactless by the same customer should alert staff as being unusual activity and the possibility that the business will be liable for the loss or monies withheld.
- New floor limits were put in place by Visa on 14 October 2017. Visa transactions take a little longer to clear, due to "live" data calculating if the customer has sufficient funds to make the appropriate transactions. If the customer doesn't have enough funds, the contactless card will come up as "declined". If the customer decides to try chip and pin, the card will also be declined. This, therefore, means the retailer bears no risk. Whilst the NFRN expects all acquirers to have followed Visa's lead, Mastercard has not confirmed their movement and AMEX is currently consulting on how they will enhance security.
- Until Mastercard and other Acquirers have enhanced their contactless security retailers need to be aware of the following possibilities:
  - A customer that has exceeded their credit/debit card limit may resort to splitting their purchases to fall below the contactless £30 limit and make high volume contactless transactions in a retailer store.

CREDIT CARD FRAUD PREVENTION

NFRN
Federation of Independent Retailers

- Retailers should be alert to "unusual" activity eg high volume contactless transactions by the same customer.
- Retailers should be particularly alert to the same customer making a £1 transaction via chip and pin then reverting to contactless.
- Whilst contactless is up to £30 and can be used up to 5 times prior to chip and pin being prompted, there has been occasions when unreasonable contactless transactions have been made and the customer used the chip and pin for £1 or the ATM for £10 before resorting back to contactless and continuing his unreasonable activity. Only the fraudster could reveal if they used their own card for the £1 and £10 chip and pin transactions and then resorted to a different stolen card.
- Where unreasonable contactless transactions arise, staff should ask the customer to pay by chip and pin facility OR suggest they withdraw money from the ATM machine to pay for their products.
- Stolen credit/debit cards are used for cigarettes, alcohol, lottery BUT also for top shelf magazines, deodorants, shavers etc (items that can be turned into cash and easily sold).
- Fraudsters tend to blend with customers at busy times of the day, when staff are busy checking through transactions and keeping the queue moving.
- Most customers tend to carry their credit/debit cards safely in wallets and normally cards only come out towards the end of the products being checked out. Staff should be on alert if the card is isolated in the hand for speedy payment (we appreciate this may not always be the case).
- If the card is foreign in origin, request chip and pin or direct the customer to the ATM.
- Cash request should only be provided through the usage of chip and pin facility.

EVIDENCE SUGGESTS

» **That the fraudster will perform contactless on small transaction figures in order that banks will not detect unusual activity within an account and that fraud could go unnoticed within the 30 day credit billing period before the account holder may notice.**

» **If multiple transactions are happening by the same customer the retailer needs to alert staff to only offer the chip and pin facility.**

» **UV note detectors will be able to identify fake credit/debit cards.**

» **The majority of your business is face to face and you may deal with cards from other countries that are mag stripe only. This is common in Amercian-issued cards and requires you to take extra precautions during a sale, such as matching card numbers and expiry dates to receipts.**

CCTV

» **Retailers need to ensure that CCTV cameras are fully operational at the till point and outside the premises to monitor or provide evidence should they become the victim of fraudulent card activity.**

» **Intelligent data can monitor the EPOS data for repetitive multiple purchases against credit/debit card transactions and focus the CCTV on the person as they enter and leave the business.**

» **It would be a good investment to have your business registered for CCTV data protection should there be a need to monitor a specific person/people within your store. The evidence that you produce thereafter will be credible should you need to prove your innocence.**

CREDIT CARD FRAUD PREVENTION

NFRN
Federation of Independent Retailers

BANKS WITHHOLDING MONEY

- Whilst each case has to be treated on its own merits, the bank will hold on to funds until the expiry of the chargeback period (normally 120 days). The bank may request receipts and CCTV material prior to returning the funds.
- Evidence suggests that a number of retailers have had their terminal contract terminated, following an investigation and being deemed outside of the risk appetite. Additionally the money the retailer was due to receive (for the sale of goods) was withheld permanently. Breaches of the contract can fall under any of the following points:
  1. To be disreputable or capable of damaging the reputation or that of any card scheme, other payments organisation or financial institution or
  2. To be detrimental to the systems, business or that of any card scheme, other payments organisation or other financial institution or
  3. May or does give rise to fraud or any other criminal activity or suspicion of fraud or other criminal activity or
  4. May or does give rise to increase risk of loss or liability to us
  5. May affect your ability or willingness to comply with all or any of your obligations or liabilities under the agreement or
  6. To be or be for a purpose contrary to applicable law and/or any policy of in relation to applicable law.

PCI DSS

PCI DSS is an acronym for "Payment Card Industry Data Security Standard" which is the security controls and processes required for the protection of credit and debit card payments through businesses.

Handling sensitive information from card payments is a large responsibility in the context of securing data. It is imperative that retailers comply with the PCI DSS standards in order to safeguard their business from any possible security breaches.

Whilst many PDQ (Pass Data Quickly) terminals are already PCI DSS enabled through their merchant acquirer, and retailers pay a monthly fee for security support, all retailers must comply with the annual validation process by carrying out an on-line assessment. Retailers paying the monthly fee can obtain Helpline support to complete the on-line assessment from their merchant acquirer.

More recently, retailers have expressed their confidence in complying with the annual assessment without any merchant acquirer support and believe the monthly PCI DSS fee is an unnecessary business cost. Whilst some merchant acquirers expect retailers to pay a mandatory PCI DSS, the NFRN encourage retailers to ask their merchant enquirer to explain what exactly is covered by the monthly PCI DSS fee.

Credit Card fraud in 2015 amounted to £575m which was a 26% increase on loss in 2014 *(statistical information from Barclay's bank).*