

TOP 10 TYPES OF FRAUD

1. ID Fraud / Identity Theft:

Dishonest individuals or syndicates will gather their victim's personal details in order to gain financial or other benefits. The victim is often left with large debt, a negative credit history and in some cases there are legal implications.

Identity theft or impersonation fraud, an existing identity is stolen/used; and **identity fraud**, a new identity is created/used

How to get ID: Burglary, Bin Raiding, Shoulder-Surfing, Skimming Cards, Spoof Letters, Advance Fee, Lottery Fraud

Figures:

- in the UK, 1 ID Theft every 4 minutes according to 2004 CIFAS figures
- 2005 KPMG Fraud Barometer reached £942m
- All fraud cost the UK economy £13.8 billion in 2002 (Cabinet Office figures, 2003)
- Norwich Union estimated that fraud cost the UK Economy around £16 billion in 2005
- Identity fraud cost the economy £1.3 billion in 2002(Cabinet Office figures, 2003)
- Estimated cost of Identity Theft reached £1.72 billion in 2005 according to the Home Office.

2. Sleeper Account:

Fraudsters will open new accounts with the intention of taking funds at a later date by simulating normal banking activity. In this way, they build a credit history and may be rewarded through access to increased credit limit, overdraft facilities and bank loan. The climax of the 'Sleeper' phase is called the "Bust-Out" whereby the fraudster dramatically increases their spending activities and/or acquires additional credit facilities and then disappears, leaving a host of balances unpaid.

3. Account Takeover:

Tricksters establishes control over an existing financial account; either a deposit or credit account, without the authority of neither the legitimate account holder nor the mandate to make subsequent transactions. Account takeover is one of the more prevalent forms of identity theft. It occurs when a fraudster obtains an individual's personal information such as account number, and alters their victim's official mailing address with the financial institution. Next, the

fraudster will call and report your card lost or stolen and request a new card replacement. The new card is then sent to the new billing address on the account. The fraudster has successfully taken over your account - hence the term "account takeover". This is currently the most popular type of credit card fraud. It doesn't require the technology of a counterfeit card, or the waiting time of a fraudulent application.

Reducing exposure is best accomplished through a combined approach of Process, Consumer Education, and Technology.

Figures:

- APACS Figures on Card's Account Takeover: £6.6m in 01, £14.9m in 03, £23.8m in 04

4. Card-not-present Fraud:

Fraudulent card crimes committed without the user of a card being present to complete the transaction (e.g. mail order, telephone and online purchases) are on the increase.

Figures:

- 1st type of Card fraud in UK: £4.6m in 95, £29.3m in 99, £150.8m in 04

Total Card Fraud Figures:

- 1 in 3 people in the UK have been affected by card fraud
- An incidence of card fraud takes place on average every 8 seconds in the UK.

5. Counterfeit Card:

Fraud committed using a counterfeit card on which the exact information of a genuine customer is embedded. It occurs after the victim's original cards have been cloned or 'skimmed', whereby sensitive banking information is transferred and encoded onto the fake cards.

Figures:

- 2nd highest type of Card fraud in UK: £7.7m in 95, £50.3m in 99, £129.7m in 04

6. ATM Fraud:

Cash Machine crime was the fastest growing form of card fraud in 2003-2004. Fraudsters target cash machines and ATM using skimming devices (see Card Skimming Fraud), which copy card details, shoulder-surfing, trapping devices (such as the Lebanese Loop Scam which resurfaced recently at Waitrose's ATMs) and miniature camera devices, which record cardholders' PINs.

Chip and pin cards aim to cut fraud by including a smart chip, which can store more information than the usual magnetic strips, and also by having users verify transactions by keying in a pin number rather than signing a receipt. France pioneered the technology more than 10 years ago - reportedly cutting fraud by almost 80% as a result.

Figures:

- APACS: only 15% of total plastic card fraud losses – £3.5m in 95, £12.2m in 99, £74.6m in 04

7. Card Skimming Fraud:

An Electronic method of capturing a victim's personal information is widely being used by identities thieves. The skimmer is a small device that scans a credit card and retrieves the sensitive information stored in the magnetic stripe. At cash machines, a skimming device is attached to the card entry slot. The device records the electronic details from the magnetic stripe of genuine cards as they are inserted into the cash machine. In addition, a miniature camera is hidden overlooking the PIN pad. This enables the criminal to produce a counterfeit card and withdraw money at a cash machine using the legitimate PIN code.

Credit card skimming often occurs in businesses where credit cards are used regularly and removed from the customer's sight in order to process payments, such as restaurants and other entertainment venues. In restaurants you will normally lose sight of your card when the waiter takes it to pay your bill. Some skimmers are as small as your hand, which makes it extremely easy for fraudster to keep them in their pouches and pockets.

8. Check kiting:

This strategy involves opening accounts at two or more institutions and using "the float time" of available funds to create fraudulent balances. This fraud has become easier in recent years due to new regulations requiring banks to make funds available sooner, combined with increasingly competitive banking practices. For example, a cheque is deposited into an account but before the cash is collected by the bank, a cheque is written against the same account and deposited into a second account, or cashed. The increased use of wire transfers allows this type of scheme to be perpetrated very quickly.

It has been estimated that the annual losses due to check fraud are in the millions of pounds and continue to grow steadily as criminals continue to seek ways to earn a living by defrauding others. For the consumer, the amount of inconvenience and anxiety caused by resolving problems with the account, local merchants, as well as possible repercussions with credit bureaus can be considerable.



9. Phishing:

A technique used to gain personal information for purposes of identity theft, using fraudulent email messages that appear to come from legitimate businesses. These authentic-looking messages are designed to trick recipients into divulging personal information and sensitive data such as account numbers and passwords, credit card numbers and Social Security numbers, PIN, e-PIN or T-PIN, Card Verification Value (CVV2), ATM/Debit or Credit Card numbers. Even if the personal information sought by the fraudsters is not provided, simply clicking on the link initiate background installations of key logging software or viruses

10. Pharming:

Similar in nature to e-mail phishing, pharming seeks to obtain personal or private; usually financial related information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof websites which appear legitimate, pharming poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. The victim's browser, however, will declare that the correct website has been accessed, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.