

CARD & PAYMENTS FRAUD GLOSSARY

Bust-out

Act of abandoning overdrawn accounts, loans, mortgages in First Party fraud.

Card-not-present (CNP)

Losses occurred as a result of card numbers being used to undertaken transactions within the electronic commerce and mail order, telephone order (MOTO) environments. CNP these days requires CVV2 number on back of card and/or correct cardholder address information.

Card not received

Fraud loss suffered on cards intercepted between manufacture/ personalisation by the card issuer and delivery to the customer.

Counterfeit

Fraud undertaken using fraudulently manufactured cards at physical merchants.

Cross-border fraud

Fraud occurring (on a card/account) in a country other than that where the card is issued.

Cross-border fraud (ATM)

Currently increasing because European cards are being skimmed at POS or ATM in Europe, then card details transmitted overseas to create white plastic or counterfeit cards for use in ATM where Chip & PIN is not implemented

First Party fraud

Deliberate setting up of account(s) with the intention of building up a level of debt that will never be repaid.

Identity Theft

Obtaining information to either attack the accounts of a legitimate account holder, to open accounts pretending to be that person, or using composite information to create fictional identities that can be used to open accounts

Insider fraud

Identity theft, data compromise or fraud involving staff inside an organisation. May involve approaches outside work to sell confidential information about their bank's customers, but coercion methods include kidnapping staff or their families, direct threats or blackmail, other coercion (friends & family connections), bribery or employee's own initiative through greed or need).

Lebanese Loop

Device made from plastic, wire or videotape that traps a customer's card in the card reader slot of an ATM but prevents a proper transaction from starting. This allows the thief to (a) shoulder surf the customer's PIN while they repeatedly try to enter PIN, and (b) steal the card after the customer gives up trying to retrieve his/her card and leaves.

Lost / stolen

Losses incurred on cards either lost by or stolen from the genuine cardholder.

'Phishing'

A general term for criminals' creation and use of e-mails and websites – designed to look like e-mails and websites of well known legitimate businesses, financial institutions, and government agencies – in order to deceive Internet users into

disclosing their *bank and financial account information or other personal data such as usernames and passwords*.

The "phishers" then take that information and use it for criminal purposes, such as identity theft and fraud.

Mass compromise

Bulk collection of card, account or customer information that can be used to support counterfeit cards or first party fraud. A famous recent case is the TJX (TJMAXX, TKMAXX) compromise that netted card and customer name and address details for between 45.7 million (official) and 100 million (unofficial) cards. PCI DSS PABP is intended to prevent this kind of data compromise in future.

Point of Compromise

The place where card details (usually magnetic stripe by itself or now, magstripe and PIN) are obtained.

Shoulder surfing

Capturing a cardholder's PIN at ATM or POS by watching as PIN is keyed in. Increasingly achieved using hidden cameras on ATM or at point of sale, even using shops' own security cameras.

Skimmed, skimming

Copying the magnetic stripe of a card in some way, now mainly using additional or compromised card readers at point of sale or ATMs.

White plastic

Cards whose magstripe and PIN will work in an ATM or other unattended device but do not need to look like a real card (cf Counterfeit). Requires PIN to be skimmed, or shoulder-surfed.