Glossary of Fraud Terms

Account takeover: A form of identity theft whereby the fraudster obtains full control over a consumer's existing account, such as obtaining the PIN or changing the statement mailing address.

Account detection rate: The percentage of fraud cases or accounts that are detected. Since a fraud case may have more than one fraudulent transaction, this number is generally higher than the transaction detection rate.

Advances fraud: Pre-meditated credit abuse. This type of fraud can be carried out by the true consumer or as a result of identity fraud. Typically occurs across multiple accounts simultaneously such as unsecured loans or credit cards opened after a Demand Deposit Account has been established and used for a period of time. Term is generally used in the UK.

Agent fraud: Occurs when a third party involved in a financial transaction perpetrates fraud. See also broker/dealer fraud.

Application fraud: Occurs when a new credit application is submitted with fraudulent details. The fraud may be the true consumer misrepresenting details or identity fraud.

ATM fraud: Encompassing term used to describe fraud related to ATM card accounts where a card is used to immediately withdraw funds from a consumer's account using a PIN-based transaction at an ATM.

AVS: Visa's Address Verification Service that enables a merchant to check the billing address (street number and zip code) against the card issuer's mailing address for the account.

Bank Identification Number: Often referred to as a BIN, this unique number consists of a two-part code that is assigned to banks and savings associations for identification. The first part shows the location and the second part identifies the bank itself.

Broker/dealer fraud: Occurs when a third party agent involved in a financial transaction perpetrates fraud. Examples include auto dealers who submit false credit applications in order to sell a vehicle or mortgage brokers who encourage consumers to falsify information on their applications in order to be approved. May also be referred to as agent fraud.

Bust-out fraud: When fraud occurs on an account that has generally been opened for a short time. The account appears to be a good account until suddenly the limit is raised, charged up and then does not pay. Differs from account takeover since is generally intended by and carried out by the original account holder. Term is generally used in the US.

Card-not-present (CNP): A transaction where the card is not present at the time of the purchase, such as for Internet, mail or telephone orders.

Case management: System that provides the facility to assign and prioritize transactions for review and action on suspect cases.

Chargeback: A credit card transaction that is billed back to the merchant after the sale has been settled. Results when a cardholder disputes a transaction to the issuer who then initiates on the cardholder's behalf.

Check fraud: Encompassing term used to describe fraud related to checks, including kiting, counterfeiting, forgery and paperhanging.

Collusion: An agreement between two or more people to participate in illegal activity for profit.

Consumer loan fraud: Encompassing term used to describe application fraud related to consumer loans.

Counterfeit: A fake card that has been created by fraudsters using stolen card numbers.

Credit abuse: Encompassing term used to describe fraudulent acts by the true consumer such as misrepresenting application details in order to obtain credit.

Credit card generators: Programs used by criminal organizations to generate valid credit card numbers that will successfully process for a transaction yet are not actual issued card numbers. Numbers are generated based on the institution's BIN and sequences numbers, and also follow the MOD-10 rules.

Credit card fraud: Encompassing term used to describe fraud related to credit card accounts where a card is used without the intention of paying for the bill or transaction.

Criminal organization: A group of individuals who collude together to commit fraud. See also fraud ring.

Current account fraud: Term used primarily in the UK. See Demand Deposit Account Fraud.

CVC: The generic term for a card verification or personal security code tied to a credit or debit card. This unique 3 or 4-digit number appears only on the card in a non-embossed format and is used for verification purposes. It ensures the actual card is in the person's possession when being used for a CNP transaction. Visa refers to this code as a 'CVV2', MasterCard as a 'CVC2', American Express and Discover as a 'CID'.

Cyber-crime: Refers to fraud perpetrated on the Internet or through the use of computers.

Debit card fraud: Encompassing term used to describe fraud related to debit card accounts where a card is used to immediately withdraw funds from a consumer's account.

Demand deposit account fraud: Encompassing term used to describe fraud related to demand deposit accounts. This can include application fraud, check fraud, ATM fraud or debit card fraud. Also called current account fraud or checking account fraud.

Detection rate: The amount of fraud detected by a fraud prevention system at a given level of account reviews.

"Dumpster diving": The practice of rummaging through someone's trash to obtain personal information used to commit identity theft.

False positive: The amount of good or true accounts flagged by the fraud prevention system as fraudulent at a given level of account reviews.

First party fraud: When a legitimate consumer (often an organized group) opens an account with no intention of repayment. Being excessively over-limit or maximizing activity on multiple accounts (i.e. checking, credit card, personal loan) are common behaviors.

Forgery: The process of making or adapting documents, such as a check, with the intent to deceive.

Fraud: A theft, concealment and conversion to personal gain of another's money, assets or information.

Fraud ring (see criminal organization): A group of individuals who collude together to commit fraud.

Fraudster: A person who commits a fraud.

Ghost terminal: Skimming device where a fake ATM touch pad and reader are placed over a legitimate ATM. Reader obtains card information and PIN, but will not process the transaction since the legitimate ATM does not function.

Hard fraud: Type of fraud committed by criminal organizations where the intent is to defraud an organization.

Identity fraud: When a fraudster creates false personal information, or manipulates an existing identity to avoid detection, in order to obtain credit or financial reward. May also be referred to as fictitious identity fraud.

Identity theft: When someone steals or otherwise obtains your personal information that is subsequently used to either obtain credit in your name or receive some type of positive benefit, such as employment, insurance benefits or housing. Use of a person's credit card information is now also considered identity theft by the FTC. See also true name identity fraud.

Internal fraud: Encompassing term for fraud committed by someone within an organization. There are two broad categories: 1) embezzling, where cash is taken directly from the organization and 2) identity theft, where customer's personal information is sold by the employee for profit.

Internet fraud: Encompassing term used to describe fraud related to the Internet. This can include application fraud perpetrated over the Internet or card-not-present fraud.

Kiting: Using several bank accounts in different banks, making deposits and writing checks against the accounts before the deposit checks clear the banking system, creating a "float" of money out of nothing more than the lag in time while checks clear and post to their respective accounts.

Mass compromise: Term used to describe situations where massive amounts of consumer data is stolen or obtained fraudulently. Examples of when it can occur include database hacks or ATM attacks.

MOD-10 rules: The validation rules used to determine if a card number is a legitimate number for a financial institution.

Money laundering: A process whereby the origin of funds generated by illegal means is concealed by making the funds appear as though they were derived from a legitimate source.

Mortgage fraud: Encompassing term used to describe fraud related to mortgages or equity lines. This can include application fraud or collusion by parties involved in mortgage transactions such as appraisals.

Nigerian letter (also known as a 419 letter or advance fee fraud): A common fraud scheme whereby an individual is targeted to help a foreign national out of the country for a large sum of money. The official requests the victim's help with the transfer in exchange for a generous fee. The official only requires the bank account number from the victim. Instead, the bank account is generally emptied. Variations include receiving a large inheritance from an unknown deceased distant relative for a 'finder's fee'.

Neural network: A sophisticated device, modeled after the human brain, in which several interconnected elements process information simultaneously, adapting and learning from past patterns.

Paperhanging: Type of check fraud where checks are written on closed accounts.

Payment fraud: Occurs when a single transaction made on a payment card is fraudulent. May be the result of account takeover or use of a counterfeit card with the consumer's account number.

Phishing: A new form of social engineering whereby fraudsters use 'spoofed' e-mails and phony websites posing as legitimate and trusted organizations to fool recipients into divulging personal financial information that is then used to commit identity theft.

Point of compromise: Often referred to as a POC, a location that can be linked back to where multiple consumers' personal information was obtained, such as a skimming device at a restaurant.

Point of fraud: Often referred to as a POF, a location where fraud occurs, generally using stolen or counterfeit cards.

Profiles: Cardholder or merchant information that represents behavior patterns. These patterns compare historical behavior with recent patterns that correspond to legitimate and illegitimate behavior which is then used by a neural network model to improve the detection and accuracy of the scoring.

"Shoulder surfing": Observing someone using a *PIN* (*Personal Identification Number*) by covertly looking over their shoulder. New application includes using a camera phone to take pictures of card numbers.

Skimming: A common method used by fraudsters to obtain payment (credit or debit) card information. It is a small tool with a mag-stripe reader that stores the information on a payment card. Generally the card is swiped through the skimmer when making an ATM withdrawal or a purchase at a location where the consumer provides their card but does not view the transaction process, such as at a restaurant. The information is then used to create counterfeit cards or sold.

Soft fraud: Type of fraud whereby a true individual who is credit hungry manipulates or alters information on credit applications in order to be approved.

Third party fraud: Any fraud scheme which occurs without the knowledge of the person whose information is used to commit the fraud. The first two parties of the transaction are the fraudster and financial institution. The third party is the individual whose identity or credit has been compromised. This is a reachable person.

Transaction detection rate: The percentage of fraudulent transactions detected by a fraud detection system.

True name identity fraud: Identity theft where the fraudster assumes your identity to become a true imposter. Personal details are used for all types of transactions including opening and closing accounts, writing checks, buying cars or homes, purchasing goods or services, etc.

Triangle scheme: A type of auction fraud where the seller uses a buyer's credit card information to purchase the good that is being auctioned and retaining the proceeds of the auction sale.

Workstation: A graphical user interface for case management functions and workflow management tasks.