#### Fraud Waste and Abuse 2018 Update to Glossary of Terms

**Account Takeover** – Account takeover means a fraudster takes over your account by changing your PIN or address so that you can no longer access your account.

**Account Takeover via Porting** – Fraudster social engineers the mobile network operator call center to “port” ownership from victim device to himself in order to obtain mobile terminating one time passwords, or even generate outgoing communication.

**AVS** – stands for address verification, which is used to determine if the billing address on an account matches the mailing address on a credit card.

**Automatic Number Identification (ANI)** – Spoofing also known as Caller ID Spoofing: The practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station. For example, the caller ID display might display a phone number different from that of the telephone from which the call was placed. The term is commonly used to describe situations in which the motivation is considered malicious.

**Bust-out Fraud** – Bust-out fraud is when the amount of available credit is raised on otherwise-legitimate credit cards. Differs from account takeover since it is generally intended by and carried out by the original account holder.

**Call Forwarding** – Fraudster enables call forwarding on the victim’s phone in order to hijack mobile terminating voice calls from the bank that contain sensitive information (one time passwords, transaction confirmations).

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

**Chargeback** – A chargeback is the reversal of the dollar value, in whole or in part, of a particular transaction by the card issuer to the acquirer, and usually, by the merchant bank to the merchant. Chargeback’s are a big problem with consumers and merchants where many accounts of fraudulent chargeback’s lead to costly fees and fines.

**Child Identity Theft** – Child identity theft is when the victim is a minor child. Because a child or parent acting on behalf of the child is unlikely to request credit reports or try to obtain credit, the theft can go undetected for a long time.

**Credit Card Fraud** – This type of fraud is committed when a credit card is used without the intention of paying for the bill or transaction.

**Criminal Fraud** – This occurs when a fraudster provides law enforcement with another person’s name and personal information such as date of birth or Social Security Number (SSN) during an investigation or upon arrest.

**Dark Web** – the portion of the Internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser. People who access and utilize the Dark Web want to browse anonymously. There’s a lot of legitimate people on it, and also bad. For example, law enforcement or journalists may use it to keep in contact with informants and others may use it to simply protect their identity from state and private surveillance. On the other hand, unfortunately, criminals also use the dark web for a variety of mischievous purposes. A fraudster might be searching for identities to purchase, or criminals might be looking to buy drugs, hacking tutorials, adult entertainment or other malicious services.

**Deep Web** – the portion of the Internet that is hidden from conventional search engines, as by encryption. The Deep Web includes the Dark Web, but also includes all user databases, webmail pages, registration-required web forums and pages behind paywalls.

**Device Cloning** – Fraudster makes a software image of the device in order to impersonate the device from a software perspective and fool device fingerprinting solutions.

**Dirty Data** – can contain such mistakes as spelling or punctuation, incorrect data associated with a field, incomplete or outdated data or even data that is duplicated in the database.

**Dumpster Diving** – The act of rummaging through someone’s trash to obtain personal information used to commit identity theft.

**False Positive** – This is the amount of good or true accounts flagged by the fraud prevention system as fraudulent.

**Familiar Fraud** – Familiar fraud in the identity industry is when your ex-husband/wife or someone close to you, like a relative, impersonates you to get access to sensitive information. This is a big issue in the healthcare industry for HIPPA compliance reasons.  An example of this would be something like an ex-spouse gaining access to your medical information.

**Financial Fraud** – Financial fraud is fraud that involves a financial account or transaction such as a bank account including a consumer loan or a credit card account.

**Fraud** – A deliberate misrepresentation to gain another’s money, assets or information.

**Fraud Prevention** – Fraud prevention is taking the steps that best protect against identity theft and other external threats targeting companies.

**Fraud Ring** – A group of individuals who scheme together to commit fraud.

**Fraudster** – A person who commits a fraud.

**Friendly Fraud** – Friendly fraud, also known as friendly fraud chargeback, is a credit card industry term used to describe a consumer who makes an Internet purchase with his/her own credit card and then issues a chargeback through his/her card provider after receiving the goods or services.

**Honeypot** – a decoy computer system for trapping hackers or tracking unconventional or new hacking methods. Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet.

**Identity Theft** – Identity theft is a form of fraud or cheating of another person’s identity in which someone pretends to be someone else by assuming that person’s identity.  This typically occurs when a person is trying to access resources or obtain credit and other benefits in that person’s name.

**Invisible Internet Project (I2P)** – an overlay network and dark net that allows applications to send messages to each other pseudonymously and securely.

**Malware** – Any software or computer program that is designed to intentionally damage or disable computers or computer systems.  Malware examples are computer viruses, trojan horses, and spyware.

**Man-in-the-Middle Attack** – an attack where the fraudster secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

**Medical Fraud** – Medical Fraud occurs when someone steals your personal information to obtain medical care, buy prescription drugs, or submit fake billings to medicare in your name.

**Payment Fraud** – This occurs when a single transaction made on a payment card is fraudulent.

**Perfect Identity** – contains enough personal information on a consumer for a fraudster to accurately impersonate that individual (Ex: Name, Address, DOB and SSN) and attempt to open and access financial accounts, file a tax return, submit a medical claim and more. This data is usually stolen information from widespread data breaches, as well as other identity theft schemes.

**Pharming** – Pharming is a type of online scam where an attempt is made to redirect a website’s traffic to another, fraudulent website.  This is very similar to phishing, however, instead of relying completely on users clicking on a link in a fake email message, pharming re-directs victims to the fraudulent website even if they type the right web address of their bank or other online service into their web browser.

**Phishing** – Phishing is a fraudulent attempt to acquire sensitive information.  This is usually done through email in which the fraudster sends out a legitimate-looking email in an attempt to gather personal and financial information from recipients such as credit card number, social security number, account number or password. Phishing emails usually appear to come from a well-known organization.

**Phoneypot** – a telephone honeypot that allows researchers to collect data from millions of calls to unlisted numbers such as robo-callers, debt collectors and telemarketers.

**Risk Management** – Risk management involves identifying, assessing, managing and controlling potential events or situations, then taking measures to control or reduce them. And with fraudsters attempting new tricks every day, being able to quickly meet the rapidly changing fraud landscape is a necessity.  This is why IDology offers easy-to-use, completely customizable technology that you can control.

**Shoulder Surfing** – This is the act of a person sneakily looking over the should of someone using a PIN.

**SMS Intercept** – When a fraudster intercepts inbound SMS communication. Fraudsters usually do this by phone cloning (lets you intercept incoming messages and send outgoing ones as if your phone were the original). If both phones are near the same broadcast tower, you can also listen in on calls.

**Skimming** – Skimming is a method that fraudsters use to illegally obtain credit card information. This is done using a method of using a small electronic device called a skimmer, to swipe and store hundreds of victim’s credit card numbers. This has become very popular at the gas pump. Fraudsters are tampering with pumps, installing skimmers and then using Bluetooth devices to read the card data.

**SMiShing** – This is a variation on phishing in which the criminal fishes for personal data over a cell phone. Instead of receiving an email, the person gets a text message that tells him to call a toll-free number, which is answered by a bogus interactive voice-response system that tries to fool the person into providing his/her account number and password.

**SIM Cloning** – A victim’s SIM card data, which contains all of their phone’s data, is copied to fraudster’s SIM so that the fraudster can impersonate a subscriber on the network and obtain all incoming communication.

**SIM Swap** – In this type of fraud, first a fraudster will collect your personal information, such as banking account information, through phishing, vishing, smishing or any other means. The fraudster then employs tactics, such as social engineering, to call the mobile network operator and deactivate the existing users SIM as well as activate a device in their possession in order to hijack all mobile communication.

**Social engineering** – a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into giving them personal information.

**Spoofing** – Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Email spoofing is one of the best known spoofs as it is fairly simple to forge and impersonate emails. Spoofed emails may request the recipient to reply with an account number for verification or may link to malware which can infect or damage a device.

**Spear Phishing** – Phishing email that looks as if it came from someone you know.  Typically the email contains a file that when opened will infect your computer with a bot or a key logger or something equally as bad.

**Social Security Fraud** – This occurs when a fraudster uses your Social Security Number in order to get other personal information. An example of this would include applying for more credit in your name and not paying the bills.

**Synthetic Fraud** – A type of ID fraud in which fraudsters combine real and fake identifying information to create new identities by either establishing new accounts with fictional identities or creating new identities from totally fake information.

**Tor (anonymity network)** – free software for enabling anonymous communication. The name is an acronym derived from the original software project name The Onion Router. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than six thousand relays to conceal a user’s location and usage from anyone conducting network surveillance or traffic analysis.

**Virus** – A computer program that replicates itself to infect computers**.**Viruses are typically spread from one computer to another through executable code in an infected file

**Vishing** – This is a variation of phishing in which the criminal fishes for personal information or attempts to install malicious software on a computer through a video file.

**Voice Over Internet Protocol (VoIP)** – phone service over the Internet.

**Voice-mail Hack** – Fraudster breaks into victim’s voice-mail typically by searching for voice mailboxes that still have the default passwords active or have passwords with easily-guessed combinations, like 1-2-3-4. Fraudster causes mobile terminating voice one time passwords sent to phone to go to voice-mail and obtains them for fraudulent use. The fraudster can also use this tactic to make international calls.