2017 Fraud Mitigation Survey Terms & Definitions Document

Terms and Definitions for Purposes of This Survey

Select terms in the survey will allow user to hover over the term and see a definition.

Term	Definition
3D Secure	3D secure is an additional security layer using three domains and SSL technology to provide a standardized and secure method of performing transactions over the internet. It and equivalent technologies are branded under different names, e.g., Verified by Visa, MasterCard Secure Code, Amex SafeKey, J/Secure, etc.
Account Takeover	A fraudster or computer criminal poses as a genuine customer, gains control of an account, and makes unauthorized transactions.
ACH Block	A service that blocks and returns ACH debits, credits or both types of transactions to a receiving customer's account.
ACH Debit Filters	An automated solution that screens incoming ACH transactions to identify unauthorized debit transactions based on pre-established criteria.
Authentication	The process that verifies the identity or veracity of a participant, device, payment or message connected to a payment system.
Authentication and Authorization Controls to Payment Processes	Authentication is proving that the users are who they claim to be and authorization is the permission to use a resource given by the application or system owner.
Authorization	The explicit instructions, including: timing, amount, payee, source of funds and other conditions, given by the payer to the payee to transfer funds on a one-time or recurring basis.
Business Email Compromise	A sophisticated scam targeting businesses, carried out by compromising legitimate business e-mail accounts through social engineering, spoofing, or computer intrusion techniques. The email may request an urgent/confidential payment, change invoice payment instructions, or other variations of the scam. The fraudsters will often use the payment method most commonly associated with their victim's normal business practices. Example - Email account of c-suite executive is compromised (spoofed or hacked). A request for a wire transfer from the compromised email ("urgent & confidential") is made to a second employee within the company who is normally responsible for processing these requests.
Carding	Testing card account number and data to confirm it is associated with a valid card number before escalating an attack or selling data. Typically transactions are low in value to avoid detection.
CIP	Customer Identification Program (CIP) as required by regulation and is the collection and analysis of basic identity information.
Collateral	Something pledged as security for repayment of a loan or credit, to be forfeited in the event of a default.
Common Point of Compromise	Potential or known point of compromise for multiple card holders is identified, e.g., at an ATM, POS or a merchant or processors database. Proactive steps can be taken to prevent further fraud losses by elevating monitoring of cards used at the common point of compromise.
Credential	A verifiable set of data presented by a participant to the payment system as evidence of identity.
Credit Underwriting	The process by which a financial organization decides to accept the risk of lending to a particular person or company.
Dedicated Computer	Computer used for a single purpose. A dedicated computer for payment processing cannot be used for other purposes like ordering offices supplies, using email, web browsing, etc.

Device Finger Printing	Information collected about an online computing device for the purpose of unique identification of the device on subsequent visits.
Established Customers	Person/business with an existing relationship with your financial institution, e.g., account, loans, etc., that have been active for a period of time.
Fraud or Payment Fraud	An action taken with dishonest intent to take something valuable from a payment system participant. Fraudulent payments fall into four general categories: • First-party fraud: Fraud committed by an accountholder against another Entity. For example, a legitimate customer may dishonestly request a chargeback on a purchase after receiving the merchandise as agreed, or an individual may set up an account (either using his or her own identity or a synthetic identity) to purchase items on credit without intending to pay the bill in full. • Second-party fraud: A transaction made or attempted by a trusted Entity that has access to the accountholder's payment credentials. For example, a child may use a parent's credit card to make a purchase without the parent's consent. • Third-party fraud: A transaction made or attempted by an unknown Entity that is not authorized by the accountholder to use a payment instrument to make a purchase, initiate funds transfers, or withdraw cash from his or her Account. • Fraud in the inducement: Deceiving a participant about the true terms of a transaction in order to mislead the participant into making a purchase, transfer, or withdrawal that is to his or her disadvantage.
Funds Availability Hold/Delay	Delay of funds availability access by account holder. Holds may be standard or exception based. Laws, regulations and rules may govern permissible practices, e.g., Regulation CC, NACHA Rules.
Identity Theft	Also known as “true-name” identity theft. Someone steals a person’s personal information, particularly a social security number and masquerades as that person by e.g., opening credit card accounts or other loans, filing fictitious tax returns to obtain refunds, receiving medical benefits, etc., in the person’s name.
Identity Verification Services	Services to help confirm the identity of the true person during account application process Examples: Real-time decision support with score and alerts on potential or known ID fraud or dynamic knowledge based/out-of-wallet authentication
IP Address	Internet Protocol (IP) address is an identifier assigned to each computer or other device that is used to locate and identify the node in communications with other nodes on the network.
KYC	Know Your Customer. This refers to the process businesses use to verify the identity of their clients.
Logical Access Controls	Technical controls that enforce restrictions on who or what can access computing resources. Access is the ability to read, create, modify or delete records, files, execute a program, use an external connection, etc.
Money Mule	“Money mules” are people who are used to transport and launder stolen money or some kind of merchandise. Criminals may even recruit money mules to use stolen credit card information. Individuals being used as money mules may be willing participants; however, many money mules are not aware that they are being used to commit fraud.
Multi-Factor Authentication	The use and validation of two or more factors for authentication. Authentication factor examples: 1. Something the participant knows (e.g., a personal identification number) 2. Something the participant has (e.g., a card or mobile device) 3. Something that is an attribute of the participant (e.g., a fingerprint)
New Customer	Person/business with no existing relationship with your organization, e.g., no account, no loans, etc.
OFAC	Office of Foreign Assets Control
Out of Band Authentication	User authentication over a network or channel separate from the primary network or channel used in transaction, e.g., online transaction with a telephone call back.

Pharming	A cyber-attack where malicious code is installed on a computer or server, misdirecting user to a fraudulent website without their knowledge.
Physical Access Controls	Controls that limit physical access to a place or resource such as restricted access or locked room where payment processes are performed, using a safe for storage of blank check stock, etc.
Phishing	A technique used, often through e-mail but may be through telephone or other means, to masquerade as a trusted party to induce individuals to reveal personal or confidential information, such as passwords.
Positive Pay Services	An anti-fraud service that helps detect fraudulent checks (or ACH debits) at the point of presentment (or receipt) and prevents them from being paid. For example, company sends a list of checks issued to its bank, which may include check number, date, amount and even the payee. When a check is presented to the bank for payment, the information on the check is compared to data from the company. Items that do not match may be reviewed by the company for a decision to pay or return it.
Post no check services	A service that blocks and returns checks on a receiving customer/payer's account. Account may be designated for use with other payment products, e.g., wires, but not checks.
Remotely Created Check	A check that is created by someone other than the person on whose account the check is drawn , often the payee or its service provider, and that does not bear the signature of the person on whose account the check is drawn.
Shared Database	A database in which multiple financial institutions contribute account and payment attributes that facilitate scoring a transaction.
Signature Verification	A technique used to validate the validity of a signature, often by comparing signatures against a previously collected signature sample. In addition to visual inspection, there are software tools that can perform signature verification. An image of a signature or a direct signature is fed into the signature verification software and compared to the signature image on file. The software generates a confidence score against the signature to be verified.
Skimmer	A device installed in a card reader or ATM that is used to illegally collect data from a credit or debit card.
Spoofing	An attack where a person or program masquerades as another with the intent to gain information. Websites, emails, telephone numbers can be spoofed.
Static Knowledge-Based Authentication	A system that maintains security questions and collects and stores answers previously provided by a customer that are used to authenticate the customer.
Synthetic Identity Theft	Synthetic identity theft occurs when someone steals a person's social security number but then uses bogus or other people's identifying information to create a person who does not exist. With a new identity, a thief may open credit card and bank accounts, get a job or otherwise use the identity to slowly create a legitimate-looking credit history. Such fraudulent activity may go unnoticed for lengthy periods because the disparate pieces of information confuse computer programs designed to match a person's information to a dataset - name, address, Social Security number, and birthdate. Instead, the system sees what appears to be a legitimate "person".
Velocity Screening	A method of screening for suspicious behavior based on counting the number of uses of a data element within a short, predetermined timeframe. The theory is the higher the number of uses on a data element the higher the risk.