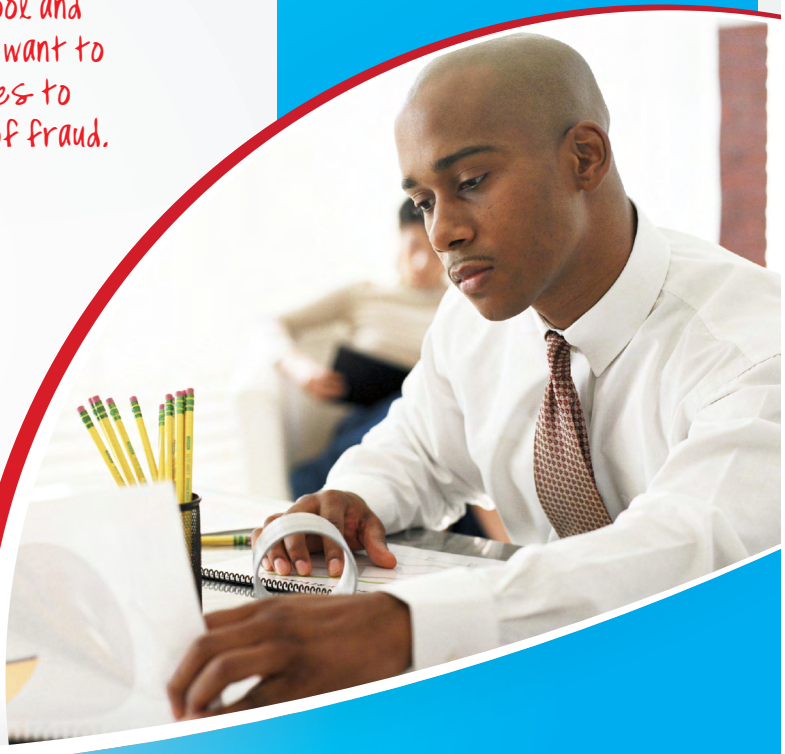
AuditLink

Glossary of Fraud Terms

Your risk mitigation team is scrambling today and when asked what is going on they tell you there has been a bust out on a members bill payment account. What in the world is a Bust out? The jargon used in loss mitigation circles describing when an account has been taken over and multiple payments are being scheduled to newly added payees. The jargon used in the auditing and compliance industry can often times be confusing and in many cases has no meaning related to the fraud activity being monitored and researched. The Audit Link Team along with a number of compliance professionals in the network have put together this document to assist you in understanding and navigating through the types of fraud frequently found in our industry.

Please use this document as a reference tool and potentially even list of activities you may want to quiz your team on processes and strategies to mitigate losses related to these types of fraud. procedures and provide ongoing training.



CU*ANSWERS Management Services

Account Takeover

A type of identity theft that involves fraud on existing financial accounts where the fraudster obtains an individual's personal information and changes the official mailing address. Once accomplished, a window of opportunity is opened for the fraudster to conduct transactions without the victim's knowledge.

Bust Out

Bill payment rule where multiple transactions have been scheduled to recently added payee(s) located either far from the individuals address or very near the subscribers address

Bust Out (Credit Cards)

Fraudster obtains a number of credit cards under false identification and runs up the balances within a few months, but never pays. These are difficult to identify as a good 'Bust Out' scheme will employ multiple banks/non-banks/credit unions as sources for credit.

CAM Alert

Proactive alerts that credit unions receive but do not always act on, which causes the alerts to result in actual fraud cases.

Check Kiting

A form of check fraud, involving taking advantage of the float to make use of non-existent funds in a checking or other bank or credit union account. In this way, instead of being used as a negotiable instrument, checks are misused as a form of credit.

Elder Abuse

The financial abuse of an elder or dependent adult occurs when a person or entity takes, appropriates, or retains real or personal property of an elder or dependent adult to a wrongful use or with intent to defraud or both.

High-Intensity Drug Trafficking Area/High-Intensity Financial Crimes Area

When completing a credit union's BSA risk assessment, the fact that a credit union's members reside and/or location exists in one of these areas elevates the risk level in the assessment.

Identity Theft

The crime of obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity in order to make transactions or purchases.

Laundering

The process of taking the proceeds of criminal activity and making them appear legal.

Money Mule

This scam involves someone offering via an email or website to pay funds into a member's account on the understanding that the member must then transfer the funds overseas generally via Western Union or a wire transfer. In return, the member supposedly gets a commission.

Placement, Layering and Integration

Money laundering usually consists of three steps: placement, layering, and integration. Placement is the depositing of funds in financial institutions or the conversion of cash into negotiable instruments. Layering involves the wire transfer of funds through a series of accounts in an attempt to hide the funds' true origins. Integration involves the movement of layered funds, which are no longer traceable to their criminal origin, into the financial world, where they are mixed with funds of legitimate origin.

Phishing

Technology or social engineering is used to entice victims to supply personal information such as account numbers, login IDs, passwords, and other verifiable information that can then be exploited for fraudulent purposes, including identity theft. Phishing is most often perpetrated through mass emails and spoofed websites.

Quick Hitter Rule

Bill payment rule where multiple payments have been made to the same payee

Single Point of Purchase

The ability to detect where a members plastic may have been compromised when the institution is experiencing a high volume of fraudulent transactions or compromised alerts across multiple memberships.

Skimming Device Fraud

Occurs when an ATM is compromised by a skimming device, a card reader which can be disguised to look like a part of the machine. The card reader saves the users' card number and pin code, which is then replicated into a counterfeit copy for theft.

SMURF cash deposits

A person who cleans ill-gotten funds by depositing cash into a financial institution and then purchasing monetary instruments that are then deposited into another financial institution. This is done to conceal the origin of the funds.

Social Engineering

A type of "confidence trick" used for the purpose of information gathering, fraud or gaining computer system access.

Straw Buyer (Mortgage Fraud)

A person who pretends to be a legitimate buyer but is actually purchasing on behalf of another person. Often, the real buyer is unable to make the purchase for himself due to a poor credit rating, so he approaches the straw buyer to purchase the goods for him and compensates him for the use of his good credit standing.

Structuring / Micro-Structuring

Term used to describe illegal transaction activity in which the member is making deposits less than $10,000 over multiple days or accounts to avoid having a currency transaction report filed on them

Title Washing

An activity where a criminal takes a vehicle title to the Secretary of State and has forged the lien release of the credit union in an effort to obtain a clear title. This title is then used as collateral on another loan at another financial institution. In some cases, it has been found that more than four credit unions believe they have a solid lien on one vehicle.

Velocity

The concept that transaction volume through a specific origin is rising at a rate which far exceeds the members average volumes. Velocity is measured by member, product, and in some cases geography. Lack thereof can also be measured relative to fraudulent activity. As an example a dormant VISA account followed by numerous web based transactions.

Wire Fraud

Frequently wiring money quickly from one account to another, often in a foreign country, through a bank or credit union, Western Union, MoneyGram, or similar business.

Who We Are

Audit Link is your execution arm for tackling auditing and compliance-related requirements and the supporting core system processes driving your operations. Credit Unions that work with Audit Link gain confidence knowing they have implemented effective procedures and controls to be in compliance with regulatory requirements.

Discover More

Visit us online at: auditlink.cuanswers.com to learn more about our offered products and services, or call 800-327-3478 and ask to speak with an Audit Link Advisor today!

AuditLink

Discover more!

Audit Link
CU*Answers Management Services
6000 28th Street SE
Grand Rapids, Michigan 49525
(800) 327-3478

auditlink.cuanswers.com

CU*ANSWERS Management Services

Proud Member of the cuasterisk.com Network