velera

Consumer-Engaged Fraud Classification Guide

030325 •

Table of Contents

Introduction

Consumer-engaged fraud has become the biggest driver of fraud losses for financial institutions and merchants. Over two-thirds of financial institutions reported an increase in consumer engaged fraud, with 35% experiencing over 1,000 fraud attempts annually (Alloy). Due to the prevalence of consumer-engaged fraud, the Velera Risk Solutions team has constructed a classification guide that outlines the various categories of consumer-engaged fraud types with clear definitions and use-case examples to aid in accurately measuring, detecting and preventing this type of fraud at your respective financial institutions.

This fraud classification guide is a critical resource for financial institution fraud teams, because it equips them with the necessary knowledge to identify and categorize fraudulent activities accurately. By providing detailed descriptions and examples of various fraud types, the guide ensures that staff can recognize and respond to potential threats swiftly and effectively. This standardization in fraud classification helps maintain consistency in reporting and data analysis, which is crucial for developing robust fraud prevention strategies. Overall, such a guide is essential for maintaining the integrity and security of financial operations, fostering a proactive approach to fraud prevention.

Classification Types

Velera has outlined two types of consumer-engaged fraud and then further classified them to better understand their patterns and impact. Differentiating between all types requires a comprehensive understanding of whether the payment made by the authorized party was influenced with or without an outside influence/party or if the payment is a false claim (intentional fraud).

The following consumer-engaged fraud types can be classified as cases where payments are initiated by an authorized party without outside influence.

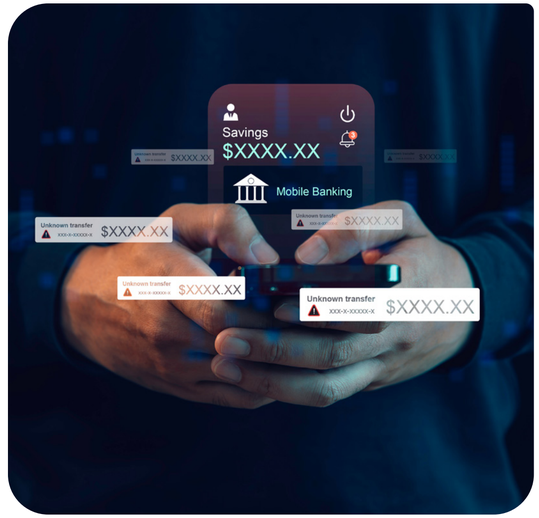
Misuse

- Authorized party (member) mistakenly or unintentionally disputes a legitimate claim. This transaction/engagement was made or initiated without outside influence. Misuse can also occur when somebody not on the account or somebody not given authority to use the account conducts a payment that is subsequentially disputed as fraud by the authorized party.
- Authorized party (member) acted fraudulently without outside influence. The individual intentionally commits fraud by disputing a legitimate transaction with no desire to pay for the services/goods rendered.

The following consumer-engaged fraud type can be classified as cases where an authorized party initiates payments with outside influence.

Persuaded

- The transaction/engagement was made or initiated with outside influence by somebody not given authority to use the account. The transaction/engagement was allowed to be completed because the accountholder or authorized user of the account engaged with a third party that enticed or socially engineered them to complete a transaction/engagement.



Sub-Classifications

By further classifying the consumer-engaged fraud types, we enable the ability to better understand impact and develop detection and prevention tools associated with these classifications. While the consumer-engaged fraud types provide an umbrella (overarching) classification and define the "what," the following sub-classifications define and categorize "how" the fraud types were executed.

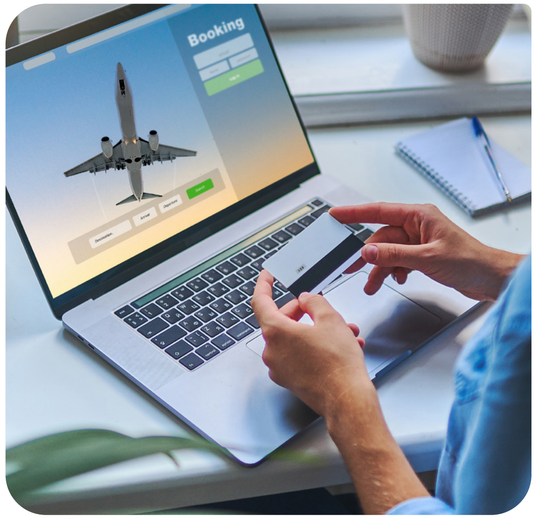
Misuse

Non-Intentional (M-NI)

A consumer reports fraud on their account because they do not recognize the transactions. However, when they are provided additional details, they know it was not fraud and assume ownership. Family/Friendly/ Authorized Use is another sub-classification of non-intentional fraud where a consumer reports fraud on their account, because they do not recognize the transaction. This transaction was completed by somebody living in their home or by somebody authorized to make the transaction.

Example: Authorized member forgets about a subscription charge for a service and disputes the transaction – reporting it as fraud. They either cannot get the merchant to cancel the subscription, or they do not remember signing up for the service. This can also include a free trial offer that they are now claiming as fraud.

Intentional/False Claim (M-FC)



A consumer reports fraud on their account for a transaction they completed or were aware of. The intention of the consumer is to not have to pay for the goods and services they purchased.

Examples:

- A person buys an expensive electronic device, uses it for a while, and then claims the transaction was fraudulent to get a refund.
- A consumer books a vacation, enjoys the trip, and then disputes the charge as fraud to avoid paying.
- A person orders a luxury item online, receives it, and then falsely claims it was never delivered to get a refund.
- An authorized user changes their mind on a product and files a fraud claim with their issuer rather than following proper dispute processes with the merchant.

Sub-Classifications (continued)

Persuaded

Pre-Payment / Investments (P-PI)

Pre-payment is when a consumer is persuaded into making upfront payments to later receive a larger payout that does not materialize.

Examples:

- Lottery winning scams where the victim is asked to pay fees upfront to claim their prize.
- A consumer is told that they have won a sweepstakes, but must pay taxes or fees upfront to receive the winnings.
- A person is promised a large inheritance from a distant relative, but must pay legal fees upfront to access the funds.

Investment fraud is when a consumer is transferring money to a fraudster under false pretenses with the expectation of a return on their investment.

Examples:

- Cryptocurrency scams where victims are promised high returns on their investments, but end up losing their money.
- Pig-butchering scams where fraudsters build a relationship with the victim and convince them to invest in fake opportunities.
- A person invests in a fake startup after being persuaded by a convincing pitch from the fraudster.

Impersonation — Financial Institution (P-FI)

Fraudsters may impersonate an employee, automated platform or digital engagement of a financial institution and convince the victim to complete an action that results in a financial loss.

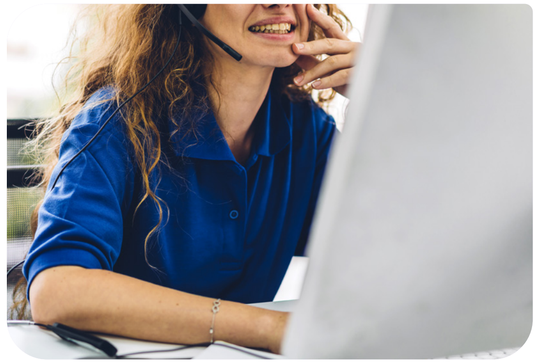
Examples:

- Fake emails that appear to be from the authorized user's financial institution, asking them to click a link to update their account information, which leads to a malicious website designed to steal their login details.
- Scammers call individuals, pretending to be financial institution representatives. They claim there is an issue with the victim's account and request sensitive information like account numbers or passwords to "resolve" the problem.
- Victims receive text messages that seem to be from their financial institution, warning them of suspicious activity on their account. The message includes a link or phone number to contact, which leads to fraudsters who then extract personal information.

Sub-Classifications (continued)

Persuaded (continued)

Impersonation — Non-Financial Institution (P-IM)



Fraudsters may impersonate law enforcement, government agencies or a family member and convince the consumer to complete a financial transaction or engagement that allows a financial transaction to take place, benefiting the fraudster. Other impersonated entities include other government institutions and employers.

Examples:

- Tax scams where fraudsters pretend to be IRS agents demanding payment for back taxes.
- Work from home (WFH) equipment scam communications to employees: Fraudsters ask employees to purchase equipment and promise reimbursement, which never happens.

Products and Services Fraud (P-PS)

The consumer initiates a payment to the fraudster for what is believed to be an authentic product or service that is later determined to be inauthentic or nonexistent.

Examples:

- Car-wrapping scams where victims are promised payment for advertising on their cars, but never receive the money.
- Rover (pet walking services) scams where fraudsters pose as pet sitters and take payments without providing any services.
- A consumer buys a high-end product online, only to receive a counterfeit or no product at all.
- A scam involving the sale of puppies, kittens or other merchandise on platforms like Facebook, where the buyer sends money through Cash App, Venmo or other peer-to-peer payment services. Consequentially, there is no puppy, kitten or merchandise being sold.

Sub-Classifications (continued)

Persuaded (continued)

Relationship and Trust Fraud (P-RT)

A consumer is manipulated into making a financial transaction to someone that they have met under false pretenses. The fraudster uses the romantic or friendly connection to socially engineer the consumer into sending funds or making purchases to benefit the fraudster.

Examples:

- Romance scams where the victim sends money to someone they believe they are in a relationship with.
- A fraudster befriends the victim online and convinces them to send money for a fake emergency.
- A scammer poses as a long-lost friend and asks for financial help, which the victim provides.

Technical Support Scams (P-TS)

Fraudsters pose as tech support to convince victims to authorize payments.

Examples:

- Device Fix Scams: Scammers claim the victim's device is infected and charge for fake services.
- Remote Access Fraud: Fraudsters ask victims to install remote access software to "resolve" an issue, then drain accounts.
- A scammer pretends to be from a well-known tech company and convinces the victim to pay for unnecessary software updates.
- Cardholders are told that their PC/laptop/phone has malware, etc. and are asked to buy gift cards to fix the problem, giving the gift card information to the fraudster.
- Common tools leveraged in this scam include: AnyDesk, TeamViewer and Microsoft ODP.

Sub-Classifications (continued)

Persuaded (continued)

Overpayment Fraud (P-OP)

Overpayment fraud is a sophisticated scam that exploits a victim's trust and creates a sense of urgency to manipulate them into transferring funds.

Example Scenario:

The fraudster pretends to issue a refund, but claims they accidentally refunded too much. The victim sees a large balance in their account, unaware it is from another account they own. The fraudster convinces the authorized party they must return the "excess refund" to avoid trouble.

Instructions to Return Funds: The fraudster directs the victim to visit their bank, withdraw the "overpaid" funds in cash, and then deposit the money into a cryptocurrency ATM. To avoid detection, the fraudster instructs the victim to lie to the bank staff about the purpose of the withdrawal, claiming it is for a personal reason or another fabricated story.

Outcome: The victim unwittingly transfers their own funds to the fraudster via the cryptocurrency ATM. By the time the fraud is discovered, the victim's money is often irretrievable due to the anonymous nature of cryptocurrency transactions.

Trending Consumer-Engaged Fraud Scams

With the proliferation of generative AI and machine-learning technological advancements, consumer-engaged fraud (similar to third-party fraud) has increasingly become more sophisticated and harder to proactively mitigate. The following chart is a reference guide documenting the most recent developments of scams impacting financial institutions with regards to consumer-engaged fraud. While these advancements can also induce second- and third-party fraud, the classifications below outline their direct impact and correlation with consumer-engaged fraud claims.

Scam Type	Description	Recent Trends/Scenarios	Relation to First-Party Fraud
AI-Generated Scam Knowledge Transfer	Generative AI as a means to create tools and methods used in schemes such as phishing emails, fake documents or strategies to manipulate authorized parties.	Usage of Generative AI engines such as ChatGPT have consequentially been leveraged to create fraud schemes and cyber-criminal knowledge transfer within the cybercriminal communities.	With the proliferation of Generative AI, authorized parties are increasingly being manipulated into authorizing illegitimate transactions of sending funds to fraudulent third parties.
AI-Generated Fake Reviews	Using AI to create fake positive reviews for products or services.	Increasing use of AI to generate convincing fake reviews on e-commerce platforms.	Fraudsters intentionally create or pay for fake reviews to boost their own product ratings, thus resulting in faulty product/ services scams.
Deepfake Identity & Impersonation Fraud	Using AI-generated deepfake videos, images or voices to create synthetic identities or impersonate a legitimate party.	Rise in deepfake technology used for creating synthetic identities for fraud. Only three seconds of a voice recording is needed to be able to replicate.	Individuals create synthetic identities to obtain credit or loans for which they would not qualify. Similarly, there are cases of authorized parties initiating payments due to interactions with impersonations of legitimate organizations proliferated via deepfake technologies.
AI-Powered Phishing	Using AI to craft highly convincing phishing emails and messages.	AI-generated phishing emails mimic legitimate communications.	Fraudsters using AI to create phishing schemes to manipulate authorized members to transferring funds or provide personally identifiable information for account impersonation or access. Authorized parties are conducting the payments with outside influence.
Voice Cloning (Deepfakes) Fraud	Using AI to clone voices for fraudulent activities.	Increase in scams using AI to clone voices of trusted individuals.	Fraudsters using cloned voices to impersonate legitimate entities and persuade authorized parties in committing fraud.

Scam Type	Description	Recent Trends/Scenarios	Relation to First-Party Fraud
AI-Driven Investment Scams	Using AI to create fake investment opportunities and manipulate victims.	Surge in AI-generated investment scams, particularly in cryptocurrency.	Consumers create fake investment opportunities to defraud others.
Automated Chargeback Fraud	Using AI to automate the process of filing false chargebacks.	Growth in AI tools that help consumers file false chargebacks.	Consumers using AI to file false chargebacks to avoid paying for goods and services.
Sophisticated Impersonation Fraud Scams via Spoofed SMS and OTP Manipulation	Fraudsters skillfully persuade authorized parties to authenticate third party access to accounts and removing fraud prevention measures built into the account.	Impersonation fraud cases have surged, involving sophisticated schemes with spoofed communications. Victims receive a spoofed SMS from their financial institution asking to verify an attempt to access an account (initiated by the third party). Believing it is genuine, they respond and report that they did not authorize the attempted transaction, leading to a follow-up call from a fraudster posing as the financial institution's fraud department. The fraudster informs the victim that to confirm their identity or to implement a fraud prevention rule, they will send a code to the victim's phone. The fraudster convinces the victim to provide a one-time password (OTP), allowing them to add the victim's card to a digital wallet. The fraudster then disables the fraud prevention measures by initiating another fraudulent transaction with a merchant, intentionally triggering a denial and generating an alert from the financial institution. A follow-up from the fraudster occurs, claiming that the denied transaction alert is a test for fraud rules. With an authenticated approval from SMS verification by the authorized party, the fraudster subsequentially has access to continually conduct unauthorized transactions, resulting in significant financial loss for the victim.	Authorized party is authenticating fraudulent transactions occurring on their accounts despite third-party manipulation.

velera

About Velera

Velera, formerly PSCU/Co-op Solutions, is the nation's premier payments credit union service organization (CUSO) and an integrated financial technology solutions provider. With over four decades of industry experience and a commitment to service excellence and innovation, the company serves more than 4,000 financial institutions throughout North America, operating with velocity to help its clients keep pace with the rapid momentum of change and fuel growth in the new era of financial services. Velera leverages its expertise and resources on behalf of credit unions and their members, offering an end-to-end product portfolio that includes payment processing, fraud and risk management, data and analytics, digital banking, instant payments, strategic consulting, collections, ATM and POS networks, shared branching and 24/7/365 member support via its contact centers.

For more information call 844.367.7728 or visit velera.com