persona

Fraud vector glossary

An overview of common fraud vectors and ways to defend against them

What is a fraud vector?

A fraud vector is a method or strategy used by fraudsters to commit fraudulent activities or exploit vulnerabilities in a system, usually for financial gain.

How do you define fraud?

Fraud comes in many forms, which vary by industry, use case, goal, scale, strategy, and endless other considerations.

At Persona, we're constantly thinking about fraud — how to detect it, fight it, and prevent it for our thousands of customers. While there are many ways to tackle this problem, we've long found that an identity-first approach is most effective. That is, we believe that the most effective way to stop fraud is to keep fraudsters from accessing your platform in the first place. By doing this, you attack the source of the problem rather than the symptoms. It's usually far better for your business to block a fraudster at onboarding, rather than catching a chargeback fraud on your platform after the damage is already done.

To keep teams up to date on the fraud types they're most likely to see, we've created this resource to summarize each fraud vector and offer strategies for defense.

The 10 most common fraud vectors
and how to stop them

Fraud vector	Description	Examples	How to solve for it
Account Creation	Account creation fraud is the act of creating duplicate or fraudulent accounts on a website or online platform, often to exploit services, launder money, or bypass security measures.	• An existing customer opens duplicate accounts to take advantage of promotions. • A bad actor leverages bots to spam users or spoof transactions.	• Government ID check • Selfie verification • Link analysis
Account Takeover	Account takeover (ATO) fraud is when an unauthorized person gains access to a legitimate user's account, such as an email, bank, social media, loyalty, or gaming account, then uses that account to commit fraud.	• A bad actor gains access to a financial account to steal funds, make unauthorized transactions, or drain bank accounts. • A bad actor hijacks e-commerce accounts to make fraudulent purchases and redeem loyalty points.	• Government ID check • Selfie verification • Reverification • Database verification • Two-factor authentication
Age Verification Fraud	An individual misrepresents their age to obtain access to age-restricted goods or services.	• An underage user attempts to have alcohol delivered, using a fake ID. • An underage user attempts to bypass security and join a gambling site.	• Government ID check • Age verification • Database verification
Business Impersonation	A person or business impersonates a legitimate business (i.e. enterprise or non-profit) using publicly available business information.	• A fraudster pretends to be a non-profit to raise funds on a crowdfunding site. • A business pretends to be a different business while going through a merchant onboarding flow.	• Government ID check • Age verification • Database verification
Identity Theft	Identity theft is the act of stealing someone's personal information, such as Social Security numbers or financial details, to commit criminal activities.	• An individual uses someone else's identity to commit fraud, such as applying for loans or credit cards with no intention of repaying them. • A bad actor uses compromised PII to open a new account or make a money transaction.	• Government ID check • Selfie verification • ID theft scores

Fraud vector	Description	Examples	How to solve for it
Marketplace Collusion	Marketplace collusion fraud happens when two entities, typically a buyer and a seller, conspire to launder and/or steal money. Fraudsters create both accounts, run stolen credit cards between them, and cash out through the seller account.	• Buyers and sellers spoof transactions on an e-commerce platform to exploit a promotional offer. • A new or small seller uses fake buyers to artificially inflate their reputations or generate more reviews.	• Passive risk signals • Link analysis
Money Laundering	Money laundering is the process of disguising the origin, identity, and destination of criminal proceeds to make them appear as if they come from a legitimate source. This often involves funds from illegal activities like terrorist financing, drug sales, or trafficking.	• "Dirty money" enters the financial system through various accounts or businesses to hide its origin, often exploiting gaps in identity verification. Once laundered, the money is reintroduced as legitimate funds, allowing it to be spent or invested without suspicion.	• KYC • Link analysis
Shell Companies	Bad actors seeking to launder money, evade taxes, or conduct illicit activity will create shell companies — businesses without active business or significant assets.	• A fraudster creates several shell companies in order to falsify transactions and therefore hide "dirty money."	• Business registrations report • Business watchlist screening
Synthetic Identity Fraud	Synthetic ID fraud occurs when someone creates a fake identity by combining real information (such as a Social Security number, or SSN) with fake personal identifiable information (PII) such as birth dates, addresses, or phone numbers, Synthetic IDs are generally used to open fraudulent accounts, access credit, or make purchases with no intent of repayment.	• A bad actor uses a fake name combined with a real SSN to apply for a credit card.	• eCBSV verification • AAMVA database check • Synthetic risk score • KYC • Link analysis
Ultimate Beneficial Owners Impersonation	Ultimate Beneficial Owners (UBO) impersonation occurs when someone pretends to be associated with a business to claim something on behalf of a business, or when they pretend to be a different individual during the Know Your Business (KYB) process.	• A fraudster impersonates a UBO by submitting falsified documents in order to open fake loans.	• KYB-KYC • Employment verification • Watchlist screening

Additional resources

The strategic guide to combating identity-related fraud

Read more →

How to protect your business against synthetic fraud

Read more →

How to protect against GenAI fraud

Read more →

Solving age verification's biggest challenges: practical strategies for a digital world

Read more →

Business impersonation:
Is your KYB strategy up to the challenge?

Read more →

How to speak ROI for fraud prevention

Read more →

To discover how Persona can help you combat fraud and safeguard your business and users, contact us. We're happy to discuss the challenges you're facing, provide a demo, and share additional resources.