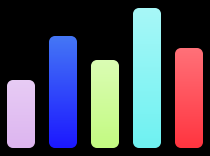
friendbuy.



How Fraudsters Game Referral Programs

Five attack vectors most programs never catch, and how enterprise brands validate every reward before money moves.

What's inside

THE COST OF FRAUD

Fraud costs a referral program in three ways. First, you pay a reward on a referral that was never real: straight cash loss the moment it happens. Second, your margin absorbs incentive liability nobody planned for, once a code or a link escapes its intended use. Third, most tools count fraud as performance, so your reporting credits referral with acquisition it never drove, and next year's budget gets set against a number that was never true.

Five vectors, mapped.

VECTOR	WHERE IT'S CAUGHT
01 · Identity fraud	Click and conversion, before any reward is created
02 · Offer leakage and arbitrage	Share and click, contained before redemption
03 · Reward abuse	Pending reward, held before release
04 · Automated fraud	Continuously, from click through payout
05 · Attribution abuse	Funnel and cohort reporting, over time

HOW FRAUD HIDES

The fraud nobody reports

Referral fraud rarely announces itself. It looks like success.

Climbing conversions. A spike in shares. A wave of new customers redeeming friend offers. The dashboard says the program is working, right up until finance starts asking why referred customers never activate, fund, retain, or purchase again.

That is what makes referral fraud uniquely dangerous. In every other channel, someone else catches the abuse. Ad platforms flag invalid traffic. Payment processors flag chargebacks. **In referral, fraud gets rewarded.** Every undetected fraudulent referral is an incentive you funded, an advocate reward you paid, and a new customer that was never real, all recorded in your reporting as performance.

If your referral tool shows you no fraud, that does not mean you have none. It means you are taking your results on faith.

Most tools look in one place, and they look too late

Basic tools check for fraud once, at payout, after everything else has already happened. **Only one of the five vectors is caught there.** By the time a reward is up for approval, the other four have already done their damage, and nothing in the system is looking back.

Identity is the first question, and most tools never get past it. **You cannot block a self-referral if you cannot tell two people apart.** You cannot confirm a referred friend is genuinely new if you cannot recognize them across devices, sessions, and the weeks between a share and a purchase.

Weak referral attribution, the linkage between an advocate and the friend they referred, fails in two directions at once:

Real advocates go uncredited.

They lose faith, stop referring, and your support queue absorbs the damage. This is the failure you hear about.

Fabricated referrals get paid.

They look identical to real ones, so nothing in the system is designed to notice. This is the failure nobody tells you about.

Basic tools rely on a cookie or a coupon. When that breaks, so does everything built on top of it.

Five vectors

Fraud tactics change constantly. The underlying vectors move far more slowly. These five account for the overwhelming majority of what we see across enterprise referral programs, and each one slips past a different gap in basic tools.

---

01 Identity fraud

One person presenting as two or more.

At the individual level, a customer opens their own referral link on a second device and collects both sides of the offer. At scale it becomes a ring: an advocate who barely exists suddenly has five referred friends, all reaching the qualifying event, none ever funding, activating, or purchasing again. The alias layer is what defeats most tools. When jane@gmail.com refers jane2@yahoo.com, an exact-match check sees two strangers. In financial services and telecom, the same person cycles alternate details to appear as several new applicants.

The cost is a double-sided payout on every instance, plus corruption of the metric enterprise teams most need to trust: verified net-new acquisition.

FRIENDBUY
Multi-device journeys, stitched together
Email signals that survive broken clicks
New-customer checks run against your own customer history

02 Offer leakage

Your referral code ends up somewhere public, and strangers start using it.

A code reaches a deal site or a cashback community, and from that moment it is not a referral offer anymore. It is a public discount, and there is no ceiling on how many people can take it. The quieter version is arbitrage: someone harvests referral links, puts them in front of customers who were already going to buy, and collects the reward on demand your brand created. Most brands find the leak in a month-end margin review, after the damage is done.

The cost is incentive you never agreed to fund, paid out to people nobody referred.

FRIENDBUY
Keeps reusable codes out of public circulation by design
Caps what any single link can pay out
Surfaces redemption spikes while they're happening, not at month end

03 Reward abuse

Collecting a reward on a conversion that does not hold.

Manufacture the qualifying event, collect the reward, reverse the outcome. Return the order. Abandon the application before it funds. Cancel after activation. Churn before the second billing cycle. The gap is the same everywhere: most tools fire the reward on the first signal that looks like success. A reward that fires instantly cannot wait to see whether the order sticks.

The cost is straight loss, with no way to claw it back once the money has moved.

FRIENDBUY
Rewards are held, not paid, until the outcome holds up
You set the window: 30 days for returns, longer for funding or activation

04 Automated fraud

Scripted abuse at a speed and volume no human pattern would produce.

Scripted clicks, mass signups, and conversion bursts can drain a program in hours rather than months. The risk climbs steeply when rewards are cash or gift cards, which are as good as money and attract organized operations rather than opportunistic customers. A tool that evaluates each referral in isolation cannot see that four hundred of them arrived in nine minutes.

These are the fastest and largest single-incident losses in referral, and the most likely to force an emergency shutdown that takes legitimate advocates down with it.

FRIENDBUY
Velocity controls hold suspicious spikes for review
Unusual click or conversion rates hold rewards until they're cleared
When abuse arrives faster than a human can react, nothing pays out by default

05 Attribution abuse

Claiming credit for sales the referral program did not cause.

The most common version runs through coupon and cashback sites, and through browser extensions that drop a referral link into the session at checkout. Unlike offer leakage, nothing here needed a discount to happen. The customer was already buying. The extension simply arrives in time to claim the credit. The same thing happens on branded search, and with links inserted late in a checkout, quote, or application flow.

No fake account is required, which is what makes this the hardest one to see. A real customer completes a real purchase, and every individual record looks legitimate. You cannot spot it in any single record. You can only spot it in the pattern: referred customers who behave exactly like organic ones, and sources that produce conversions without ever producing a single share.

Over time this is the most expensive of the five, because you are paying acquisition costs on demand you already owned.

FRIENDBUY
Tracks the referral funnel stage by stage, from share to click to conversion
Flags conversions with no journey behind them
Shows whether referred customers actually behave like referred customers

BENCHMARK YOUR PROGRAM

Why basic tools miss all five

Fraud prevention is not a feature you check off. It is a level you operate at, and most teams have never been told which one they're on.

Level 1 · Basic	Level 2 · Platform-managed	Level 3 · Integrated enterprise
Single-cookie identity	Cross-device identity resolution	Multi-signal identity, reconciled against your systems
Exact email matching only	Alias and similarity detection	Eligibility validated against your customer history
Reusable coupon codes	Single-use codes, per-link caps	Reward caps across all campaigns and time frames
Rewards fire instantly	Pending rewards with hold windows	Your systems approve each payout before it fires
Conversion = checkout only	Configurable conversion events	Any business event: funded, bound, activated, retained
No fraud visibility	Fraud caught and reported	Every verdict inspectable, with its reason, audit-ready

If your controls sit in the first column, the honest answer to "how much fraud is in our program?" is that nobody knows. Level 1 is where referral lives when it is a checkbox feature inside a platform built for something else. Level 2 works against known patterns. Level 3 is where enterprise evaluations are decided: your systems participate in every payout decision, validation is tied to the outcome your business recognizes as revenue, and every verdict can be defended to the people who will eventually ask about it.

When the conversion is not a purchase

An application is not a funded loan. An install is not a retained subscriber. A bound policy is not a renewed one.

In lending, insurance, telecom, and subscription businesses, the meaningful outcome may arrive weeks after the referral, in a different system, with no shopping cart anywhere in the journey. Reward the early signal and a referral program becomes a lead-generation bounty with a predictable incentive for abuse. Reward the validated outcome, defined by your systems, and the incentive to manufacture a proxy disappears.

INDUSTRY	THE EARLY SIGNAL DO NOT RELEASE A REWARD	THE VALIDATED OUTCOME RELEASE THE REWARD
Lending	Application submitted	Loan funded and first payment made
Insurance	Quote requested	Policy bound and first premium paid
Banking	Account opened	Account funded and active past 30 days
Telecom	Line activated	Service retained past the cancellation window
Subscription	Trial started, or app installed	First paid billing cycle completes
Ecommerce	Order placed	Order ships and the return window closes

Every row on the left is a real event your systems can see. None of them is revenue yet. **The gap between the two columns is where reward abuse lives.**

Decisions you can defend

For regulated and high-value programs, integrity is not only about blocking bad actors. It is about demonstrating control:

Your systems hold final payout authority

evaluated in real time before any reward fires

Every verdict carries an inspectable reason

whether released, held, or declined

The record is audit-ready

for whatever your finance, risk, or compliance function eventually asks

And when something does go wrong

Suspicious activity surfaces to your team automatically, and Customer Success monitors program health alongside you. When an issue needs more than monitoring, escalation runs from Customer Success to the solutions team to engineering. **Never into a ticket void.**

USE THIS IN YOUR NEXT VENDOR REVIEW

Ten questions to ask any referral platform

Strong platforms answer these in the demo. Gaps that are hard to answer during evaluation become expensive to discover after launch.

01 **Identity.** How is identity resolved across devices, long consideration windows, and multiple systems, and what happens when the cookie is gone or the click is broken?

02 **Coverage.** What fraud checks run on every referral, and which of them can we configure?

03 **Self-referral.** How do you catch it beyond identical email matching, and can eligibility be checked against our own customer or account history?

04 **Validation windows.** Can rewards be held through our window, and what happens when the outcome is later cancelled, refunded, reversed, or charged back?

05 **Payout authority.** Can our own systems approve or reject each payout in real time before it fires?

06 **Conversion events.** Can rewards be triggered by a custom business event rather than a cart purchase?

07 **Reward caps.** Can we cap total rewards per customer across all campaigns and time frames?

08 **Velocity.** How do you handle spikes in clicks, conversions, and signups, and is suspicious activity held or paid by default?

09 **Visibility.** Where do we see what fraud was caught, and the reason behind every individual rejection?

10 **After launch.** Who monitors program health with us, and what is the escalation path when something breaks?

Question five is the one worth pressing hardest. A vendor who cannot let your systems approve a payout is asking you to trust their judgment instead of yours.

How exposed is your program right now?

Most brands cannot answer that question, because the controls that would surface the answer are the ones they do not have.

We will walk through your referral journey stage by stage, show you where each of the five can get in, and show you how enterprise brands validate every reward before money moves.

Request a referral integrity review