Fraud and Platform Fraud Overview

We live in a great big world of fraud, most of it happening right under our noses, and much more frequently than we think. In 2016 more than 15 million Americans, or about 5% of the population, experienced some form of identity or credit card theft and 16% of SMBs have experienced payment fraud.

A Few Examples of Common Fraud

- Account takeover: Fraudsters use stolen account credentials to pay themselves with your credit card, or cash out funds in your account.
- Payer fraud: Fraudsters masquerade as good payers to buy goods and services with stolen credit cards. Payer fraud also includes payers buying and charging back goods they actually received.
- Fraud spikes: A fraudster finds a vulnerability or loophole for financial gain, for example finding a bug that lets them run repeated transaction rapidly under certain circumstances, and the fraudster will exploit it repeatedly, tell friends, and keep doing so until the loophole is closed.
- Compliance violations: There are a wide range of compliance issues. These include any transaction or merchant in violation of credit card or bank rules; payers and merchants on the OFAC list; sale of certain items to sanctioned countries; processing funds that are the result of money laundering; and many others. Violations can result in massive fines.

But fraud is an even bigger problem for online platform businesses where both sophisticated multi-party fraud and common payer fraud takes place.

Platform Fraud

- Merchant fraud: More sophisticated fraudsters and money launderers know that setting up a fraudulent merchant account can be harder to detect and so set up fraudulent accounts. But payers as well as merchants also go bad over time, perhaps to cover losses from poor operations, eventually disappearing or going bankrupt.

- Credit risk: A merchant could go under and leave you with liability.
- Collusion fraud: Any scenario where the payer and merchant turn out to be the same person, or working together, to defraud the platform, frequently with the payer paying the merchant account with stolen credit cards and then cashing out.
- Fraudster's choice: Fraudsters are creative, tech-savvy online criminals. They will mix and match and come up with new techniques.
- Trust and safety: Not technically fraud, however platforms are on the hook for quality of goods, services, and the legitimacy of consumers on their platform, and a failure to measure up can lead to not just chargeback fees for your merchants but penalties from card organizations due to excessive chargebacks. These issues can lead to dissatisfaction among your merchants and users.

An Even Bigger Issue: False Positives

What's a false positive? Shutting down a good merchant or transaction because it might be fraudulent. False positives are currently a much bigger problem than losses due to legitimate fraud. In 2016, false positives totaled $118B, or 13 times fraud losses. What are the consequences?

- Declined transactions are missed learning opportunities, meaning your risk management won't improve over time.
- Poor user experience will cause a drop in user retention and will earn you a reputation for being difficult to use, in turn increasing user acquisition costs.
- Monetizing fewer transactions, and missed revenue opportunities.

To find out more about managing these issues and how smart fraud solutions can balance these conflicting requirements, click here to speak with us or visit wepay.com.