The Hidden Fees of Fraud

Pattie Dillon, Product Manager, Anti-Fraud Solutions | SpyCloud

Pattie Dillon has spent 20 years in the fraud prevention, risk mitigation, and identity verification space, with roles at Etalinc, Veratad Technologies, and Wolfe. Now at SpyCloud, Pattie is the Product Manager for Anti-Fraud Solutions. Her focus is developing creative and innovative ways to fight fraud with SpyCloud's leading-edge products in an effort to make the internet a safer place to do business.
Pattie is a member of Payments Risk and Fraud Consortium.

We are all aware of lost revenue from online and offline fraud resulting in chargebacks, refunds, and issuing credits to synthetic identities. The pandemic advanced the adoption of digitization across the entire payments ecosystem. Merchants scrambled to keep their doors open by leaning heavily on e-commerce channels to begin or expand their online presence.

Throughout 2020, the explosion of online sales through existing markets was met with an equal explosion in emerging food market segments such as grocery stores, restaurants, and delivery services. The digital transaction volumes in these verticals have now grown into a vital part of their business models.

Evolving in parallel to the increased sales volume driven by the pandemic is fraud across all sectors.

A revealing Aite Group study reported 2020 Identity Theft losses of $712.4 billion, up 42% from 2019. Identity Theft is a direct result of breaches and leaks coupled with password reuse, and is the gateway to fraudulent transactions and criminal activity.

When spikes in fraudulent transactions bubble up to the surface, resolving them presents new challenges in terms of identifying how they happened and how to prevent them in the future. Depending on the industry, resolutions run the gamut from handling chargebacks and loss of merchandise to blocking the use of fraudulent prepaid cards issued to criminals using stolen credentials and identities. Some online businesses – especially government agencies – have been completely unprepared to handle the tsunami of requests and transactions, and as a result, experienced crashed servers and forced application and claim delays.

Factored into fraud losses are the expense of labor to investigate and remediate each fraud issue, brand reputation damage, and loss of customers. But wait – are you counting the hidden costs of transactions?

Interchange fees are often overlooked when calculating fraud. These fees range from 1.5% to 3%, plus another assessment fee of 0.14% of the amount of each transaction. An increase of up to 20% of Visa's interchange fees, applied to each transaction processed, was planned to take effect in April 2021. It should be noted that when Visa makes a fee change, MasterCard follows the same trend. In a statement made on March 16, both Visa and MasterCard delayed the increase by a year – but now is the time to prepare.

As you can imagine, whether it is a transaction completion or reversal, the fees add up. Visa had originally slated the interchange fee increase to go into effect in 2020 but held off due to the pandemic. A report of the annual spend of processing fee statistics totaled $180 billion per year on processing fees; $63 billion of that total is the result of errors and overcharges.

The impact of the impending interchange increase (up to 20% for some industries) means now is the time to put strategies in place to proactively prevent fraud to avoid significant hidden fees. The importance of identifying fraud before the transaction completion becomes even more critical to maintaining overall profitability.

To give you a sense of the annual revenue Visa Network generates from interchange fees for payments, as of June 2020, they processed over 140.8 billion transactions totaling $11.1 trillion in payments. That's an average of $80.00 per ticket.

Recommendations to Avoid Fraud:

Look to layer third-party anti-fraud monitoring solutions into your stack that give you the flexibility to easily pivot as fraud trends change. It's also critical to properly test and calibrate these applications for desired results. While a bit of friction is necessary to truly get ahead of cybercriminals, there is no need to substantially disrupt the customer experience in the name of fraud (and unnecessary interchange fee) prevention.

Best practices for internal fraud monitoring include:

- Account creations
    - Record average of daily and monthly creations
    - Unaccounted/unexplained spikes in creations
- Login
    - Record average number of login attempts per user
    - Abnormal amount of login attempt velocities
- Account information modifications, such as changes to:
    - Emails
    - Phone
    - Credit card information
    - Account holder address
    - Shipping address
- Account holder purchasing trends (i.e. changes in buying habits)
- Shipping instructions
    - Escalated shipping from standard to overnight
    - Mid-shipment re-routing of physical goods to a completely different address
- Noticeable trends
    - Reports from account holders or non-account holders of fraudulent activity
    - Reports of internal and external unauthorized account access
    - Spikes in new account creations
    - Spikes of customer service calls or tickets

    - Unusual spikes in web traffic
    - Properly testing and calibrating any internal business rules for desired results
- Added response for suspect transactions
    - Determine the step-up processes
    - Only push to a review processes when necessary

Especially important now are verifying the user’s entered information and monitoring for behavioral indicators identifying anomalies in the device, IP address, and phone number associated with the transaction, along with:

- Risk indicators related to the user’s breach exposure (are they using a password that has been compromised in a breach? This could mean a bad actor is behind the transaction and not a legitimate user.)
- Changes to the typical credit card type used (i.e. credit vs debit vs prepaid)

As the expense of processing fraudulent transactions and applications and issuing credit continues to rise, being vigilant and avoiding fraud while growing your business is a balancing act that takes skill and dedication. The benefit of putting energy into anti-fraud efforts is ensuring a smooth user journey for legitimate customers while securing their account information *and* your company’s profitability from hidden fraud transaction fees.

KEYWORDS: SpyCloud, Anti-Fraud, Fraud, Risk, Charge backs, refunds, synthetic identities, identity theft, AITE Group, interchange-fraud