The (True) Costs of Payment Fraud

The rapid rise of eCommerce platforms and the accompanying $861 billion spending splurge in tandem with the government's huge COVID-triggered relief packages have spurred a significant surge in payment fraud. And while losses are a major consequence, they're only part of the overall impact that fraudulent activities have on businesses.

Even before the pandemic struck early in 2020, losses from general purpose and private label credit, debit, and prepaid card fraud were already on the rise. Gross fraud losses amounted to $28.65 billion in 2019, up 2.9% from $27.85 billion in 2018. This doesn't even include the billions of dollars in fraud losses related to QR code-based and push payments.

All stakeholders—customers, vendors, financial institutions, and everyone in between—are impacted in a range of ways, and the impacts associated with payment fraud extend beyond just monetary value and include reputational, operational, and regulatory costs.

With ever-lurking fraudsters becoming increasingly sophisticated and research indicating that online sellers will lose $130 billion to online payment fraud between 2018 and 2023, it's crucial for all who form part of the payment ecosystem to adopt more rigorous fraud prevention measures and remain vigilant.

Businesses Suffer From the Costs of Payment Fraud

Fraud, naturally, drains money from businesses and merchants are among the hardest hit. On average, merchants spend between 3-5% of their revenues fighting fraud. Still, as much as 1% of orders are missed, often resulting in chargebacks that range from $15-115. The total amount of money lost by merchants due to chargebacks is anticipated to exceed $40 billion before 2025!

Chargebacks are important protections that increase public confidence in credit and debit card payments, but they present a double whammy for online retailers: After making a fraudulent purchase and then fraudulently filing a chargeback complaint, it adds insult to injury when that company must also cough up extra fees and fines as a result.

Additionally, if companies happen to exceed a defined chargeback threshold, they

could be entered into an Excessive Chargeback Program which costs them additional fees until they get their chargeback rate under control. Worse, they can be flagged as being "high-risk." Chargebacks, however, are only the proverbial tip of the iceberg as merchants also pay big time in other ways, including reputational damage and higher operational costs.

Payment Fraud Has Been Increasing During the Pandemic

Studies have found increased fraudulent activity across nearly every business category during the pandemic. The Association of Certified Fraud Examiners (ACFE) found that 77% of respondents have reported an uptick in fraud since the outbreak and expect it to continue.

While COVID-19 hasn't introduced the problem—fraud and economic crime were already at record highs pre-pandemic—it created an environment in which criminality flourished. Three conditions unique to the pandemic contributed to a distinct rise in business fraud.

Ecommerce Boom – Pandemic-driven regulations such as social distancing and quarantines have prompted consumers to spend heavily online as both customers and businesses looked to avoid physical contact. As a result, 2020 eCommerce spending touched $840 billion in annual sales.

In the gush of online transactions, scammers upped their nefarious game considerably, with 68% percent of anti-fraud professionals noticing an increase in payment fraud last year. Cybercriminals used stolen or fraudulent information and unauthorized credit cards, gift cards, and digital wallets to go on their bogus shopping sprees, leaving businesses to pick up the tab.

Federal Financial Assistance – The government passed multiple billion-dollar relief measures to help offset the economic difficulties triggered by the pandemic. A significant portion of businesses (62%) and more than 5 million individuals benefitted through this program. The sheer scale of the stimulus package combined with relatively minimal oversight of applicants created fertile ground for a fraud frenzy.

Increased Security Risks From Remote Work – While technology makes it easier for remote employees to do their jobs and stay connected, it has increased security challenges. In the dash to enable employees to work from home, many businesses relaxed security protocols and rushed the adoption of systems that would’ve otherwise been rigorously evaluated. This left business networks wide open to fraudsters. As customers, businesses, and employees scrambled to adjust to new

technologies, hackers were presented with a virtual gift, and cyber fraud escalated.

Reputation and Operational Impact on Businesses

Companies spend years painstakingly building a brand, only to lose it overnight because of a security breach. Fraud-induced reputational damage will ultimately result in losses that are far greater than just the direct financial cost of a particular fraudulent activity, and it can be difficult to measure.

Of course, the most obvious way in which fraud affects a business is financial loss, but it usually goes well beyond that. A company embroiled in fraud is usually a red flag for investors, partners, customers, and employees. Who wants to deal with entities that cannot be fully trusted?

There’s also the possibility that you can be flagged as a high-risk vendor by card networks. This will result in higher card processing fees, and in some cases, may lead to your business being blacklisted by a card network.

Fighting fraud is a time-consuming and expensive process. Employees invest long hours in investigations, settling representations, and fraud audits. All of these incur high labor costs. In addition, money spent on shipping fraudulent transactions is gone, forever, with large orders (usually heavier and more expensive to ship) more likely to be fraudulent than lighter ones. Fraud also usually triggers a rethink of the business strategy with added costs in terms of money and time.

NatPay: Your End-To-End Payment Solution

As the online payment ecosystem continues to grow, so too will the opportunities for fraudsters who continue to adjust their social engineering techniques to breach business payment systems.

The (true) cost of payment fraud is not just determined in lost dollars. Payment fraud can affect your company's reputation, its ability to operate smoothly, and even regulatory compliance. Businesses that don't manage their risks effectively may experience eroded customer confidence or complicated relations with partners.

All these side effects will have negative impacts on the growth and overall success of your business. NatPay offers secure payment solutions designed specifically for y our business ensuring that the fraud protection call from National Payment’s team of trusted analysts and payment professionals is the call you *want to get.* Have questions? We're here to help you eliminate risk while still providing flexibility in how you execute a payment. Contact us today.