The CFO's Challenge: Fighting Fraud in the Digital Age

AN E-COMMERCE WHITE PAPER

The CFO's role is evolving from its traditional position as the company's financial gate-keeper. Once solely charged with accounting and finance responsibilities, CFOs are now a key strategic partner and advisor to the CEO as they navigate a landscape with a greater — and growing — percentage of digital liabilities.

One of the top issues on the minds of most finance executives as they consider the new year is cybersecurity. With cyberattacks multiplying and the EMV liability shift moving more fraud to online channels, CFOs are expected to assume larger roles in assessing risks and developing measures to prevent security breaches while preserving and protecting revenue streams.

For CFOs working in organizations with an e-commerce channel, this concern is front and center. With e-commerce already representing more than 8.1 percent of all retail sales, these leaders must focus on reducing the complexity and mitigating the growing risks of e-commerce fraud while continuing to drive revenues. Forrester Research predicts that e-commerce sales will grow at a 10 percent compounded annual rate over the next five years to $480 billion, or nearly three percent of the U.S. GDP, and fraudulent transactions are expected to scale in tandem.

Understanding the True Cost of Fraud

CFOs need to understand the impact that soaring levels of online fraud will have on their companies' bottom lines. Merchants with an online channel are already losing 7.6 percent of their annual revenue to fraud.

Risks are especially acute for e-commerce companies, which are increasingly dealing with fraudulent transactions in card-not-present (CNP) sales. E-commerce merchants dealing exclusively in digital goods, such as electronic tickets, downloads, and gift cards, are suffering the worst hits, losing 8.6 percent of revenue on average to fraud and related costs. Hybrid goods merchants — selling both physical and digital goods — are facing similar losses at 8.1 percent of revenue.

Page 2 >

And, of course, physical goods merchants aren't getting off scot-free either. The proliferation of buy online, in-store pickup programs enables fraudsters to bypass validation checks for EMV chip protection and/or delivery to their physical address.

Fraud's Hidden Impact

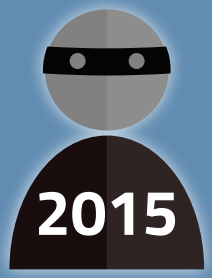
Along with direct hits to a company's bottom line, CFOs must also consider the hidden impact of fraud due to false positives, which occur when overly sensitive anti-fraud controls block good transactions from legitimate shoppers. On average, 30 percent of all transactions that get declined due to suspected fraud are believed to be legitimate.

Again, digital goods merchants face the worst plight, with 34 percent of their declined transactions believed to be legitimate. This translates into 2.8 percent of revenue lost due to false positives.

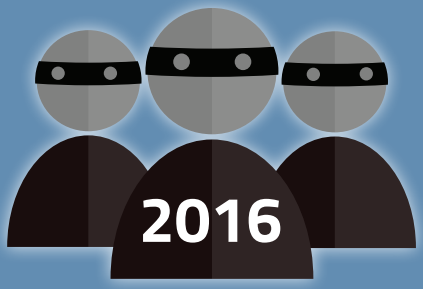
And the multiplier effects of false-positive transactions should be especially sobering to CFOs. Customers who endure the inconvenience and embarrassment of having their purchases denied at check-out report diminished loyalty to the business they had been trying to patronize. A whopping 66% of customers won't return to a business after being falsely identified as a fraudster. Add in the reputational damages to the brand and companies can face incalculable losses over time.

THE RISING TIDE OF FRAUD

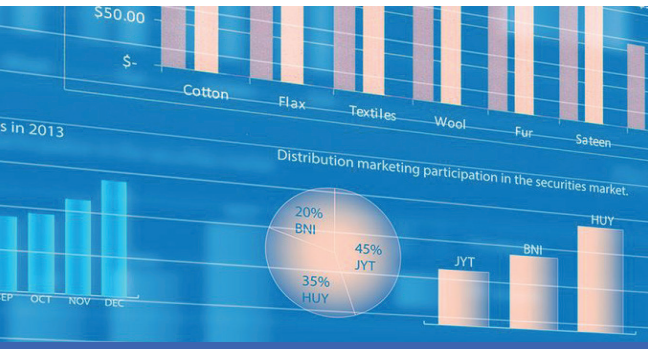
Between fraud management costs, false positives and chargeback losses, e-commerce merchants are losing a significant portion of their revenues and already tight margins.



Nearly 3 in 4 merchants dealing in both digital and physical goods said that fraud and chargebacks had a major financial impact on their business in 2015, accounting for 13 to 20 percent of their operational budgets that year. Javelin 2015



Fraud and chargeback management costs ate up even more of merchants' operating budgets in 2016, taking 14.9 to 23 percent, with digital goods merchants coming in at the top of that range. Javelin 2016



As e-commerce transactions scale, the manpower and expertise required to maintain in-house solutions will increase merchants' operational costs exponentially.

The Delayed Impact of Chargebacks

As shopping preferences continue to evolve, consumers are prioritizing credit card safety and security. The card brands have promoted a "no risk" approach to online shopping with their products, and this includes the ability to reverse (or chargeback) unintended charges. While operating as a safety net for consumers, this has also opened opportunities that many fraudsters choose to exploit.

Chargebacks usually don't hit the bottom line until 60 days after the original sale. This means that a big jump in sales volume — unrelated to seasonality or major sales — can signal that the company has been hit by fraudulent purchases and will soon start seeing a spike in chargeback losses.

When customers reverse a charge, the business must generally cover the cost of goods sold, pay bank fees, and take on operational expenses to help mitigate the ongoing threat of chargebacks. The merchant faces the risk of additional fines and fees if chargebacks reach certain thresholds that are established by the card companies.

Managing the costs and risks of chargebacks has therefore become a strategic priority for many CFOs. In-house chargeback management strategies, however, typically tighten fraud controls too severely, exacerbating the risks of declining valid sales, alienating good customers and losing legitimate business through false positives. And as e-commerce transactions scale, the manpower and expertise required to maintain in-house solutions will increase merchants' operational costs exponentially.

How Organizations Fight Fraud Today

Today, 41 percent of merchants hire and train in-house personnel to identify, respond to and resolve fraud situations. Javelin found that these staffing costs account for 36 percent to 41 percent of all fraud and chargeback-related expenses for merchants across all segments. Costs are even higher for digital goods merchants: they employ nearly five times the fraud-prevention personnel as physical goods merchants.

At the same time, 48 percent of merchants have chosen to place a greater emphasis on technology and are automating some of their fraud prevention processes. This approach requires a sophisticated understanding of the available technology: solutions need to be evaluated, purchased, integrated with other technologies, and then maintained and managed over time. As fraud threats and tactics continue to evolve, they also must be constantly recalibrated to address new risks.

For many merchants, managing fraud risk and its aftermath are tasks best left to third-party specialists — 37 percent of all merchants and 43 percent of digital goods merchants have already outsourced these services. Many of these third-party service providers have the ability to scale their technology investments and human resources in ways that are difficult for individual organizations.

Finding the Right Balance Between Security and Profitability

Both in-house and outsourced approaches require unique balances between manpower and technology as well as between protection and a fast, easy checkout process that can help drive sales. Almost every decision will require a trade-off between convenience and ease for the customer and the bottom line of the organization.

CFOs have multiple models to consider for mitigating the risk of fraud, and their decisions will, to some degree, depend on their companies' product mix: physical, digital or hybrid. But across all segments, effective fraud management calls for an understanding that there are few clear-cut "either/or" choices. It also calls for trade-offs, not only between convenience and security for the customer, but also between the fraud fighting strategies CFOs choose to execute.

Regardless of whether companies decide to bring their fraud management solutions in-house or outsource them, investments in both personnel and technology must be prioritized.

Considering the diversity in today's marketplace and merchants' unique offerings, there is no single anti-fraud investment strategy that will work for every business.

The Challenge for 2017: Scalability

Businesses are under pressure today to establish efficient and customer-friendly online capabilities in the face of intense competition from the digital giants. Yet resources that must be allocated to building, managing and maintaining in-house fraud solutions can hinder and limit the ability for merchants to scale their business or adapt to an ever-shifting landscape of risk over time. These inabilities may also damage or add friction to the customer experience, impacting revenues in ways that may initially be hard to see and correct.

Regardless of the path they choose to balance fraud management investments, CFOs will face a clear choice: Do they get into the business of fighting fraud — which will create an increasing operational cost — or do they outsource and focus on core competencies and growing their business? A compelling business case can be made for outsourcing fraud mitigation and prevention measures.

The value of turning to a third-party service provider becomes especially salient in light of the increased risks and costs projected for 2017, and beyond. Reducing the money and staff time spent can free up additional resources to drive revenue and company growth. And this, in turn, can enable CFOs to better serve as strategic advisors to their CEOs.

Americas | Europe | Asia

Visit us at trustvesta.com

11950 SW Garden Place
Portland, OR 97223-8248 USA
Tel: +1 503.790.2500
Fax: +1 503.790.2525
info@trustvesta.com

4400 Alexander Drive
Alpharetta, GA 30022-3753 USA
Tel: +1 678.222.7200
Fax: +1 770.772.0600
info@trustvesta.com

Av. Américas 1536 1A
Col. Country Club
C.P. 44637
Jalisco, México
info@trustvesta.com

Vesta Building
Finnabair Business Park
Dundalk, County Louth
Ireland A91 E934
Tel: +353 (0)42 939 4600
Fax: +353 (0)42 933 4121
info.ireland@trustvesta.com

No. 6 Ji Qing Li Road,
Unit B603
Chaoyang District, Beijing
100020 P.R. China
info@trustvesta.com