VESTA

Americas | Europe | Asia

False Positives: The Undetected Threat to Your Revenue

Merchants dedicated more of their operational costs to fighting and managing fraud in 2016 than ever before.

As virtually every merchant in 2017 knows, fraud is a big business for criminals and a serious threat to revenue. A recent study that canvassed 500 e-commerce merchants taking in $1 million or more annually—*The Financial Impact of Fraud*—revealed that merchants dedicated more of their operational costs to fighting and managing fraud in 2016 than ever before.

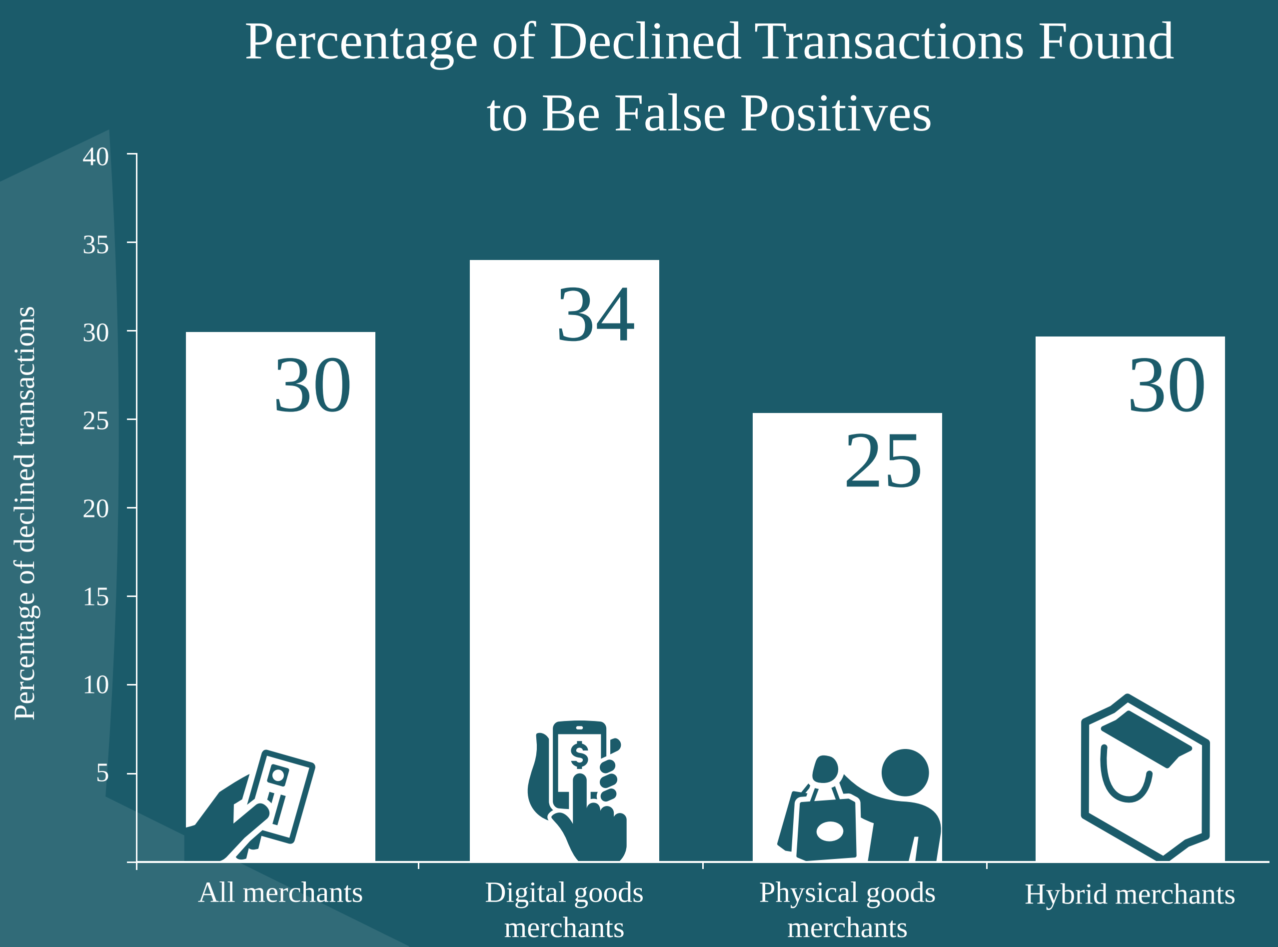
Fraud management now consumes 14.9 to 23 percent of merchants' operational budgets—up from 13 to 20 percent just a year prior. Software and hardware provide the initial tools, but human capital is required to deploy technology and calibrate fraud controls.

Perhaps worse than experiencing outright fraud, however, is losing both a transaction and a customer because the merchant's fraud controls were overly sensitive and blocked legitimate shopping activity. Transactions that are wrongly declined due to suspected fraud are known as "false positives." These undetected sales killers pose serious threats to merchant revenue and customer loyalty.

When the overall problem of fraud is broken down, the dollars lost to false positives actually eclipse the dollars lost to chargebacks by more than five to one. Merchants as a whole are losing 2.79 percent of their revenue to false positives, but are losing only 0.52 percent to chargebacks.

Looking at the different retail segments, merchants selling strictly physical goods experience the lowest false-positive losses, at 1.81 percent of annual revenue, and those who sell both physical and digital goods face the greatest losses, at 3.35 percent.

Perhaps worse than experiencing outright fraud is losing both a transaction and a customer through a false-positive decline.



1 in 3

Declines Is a False Positive

VESTA

How False Positives Complicate Fraud

Nearly a third of all transactions that are declined due to suspected fraud are believed to be legitimate.

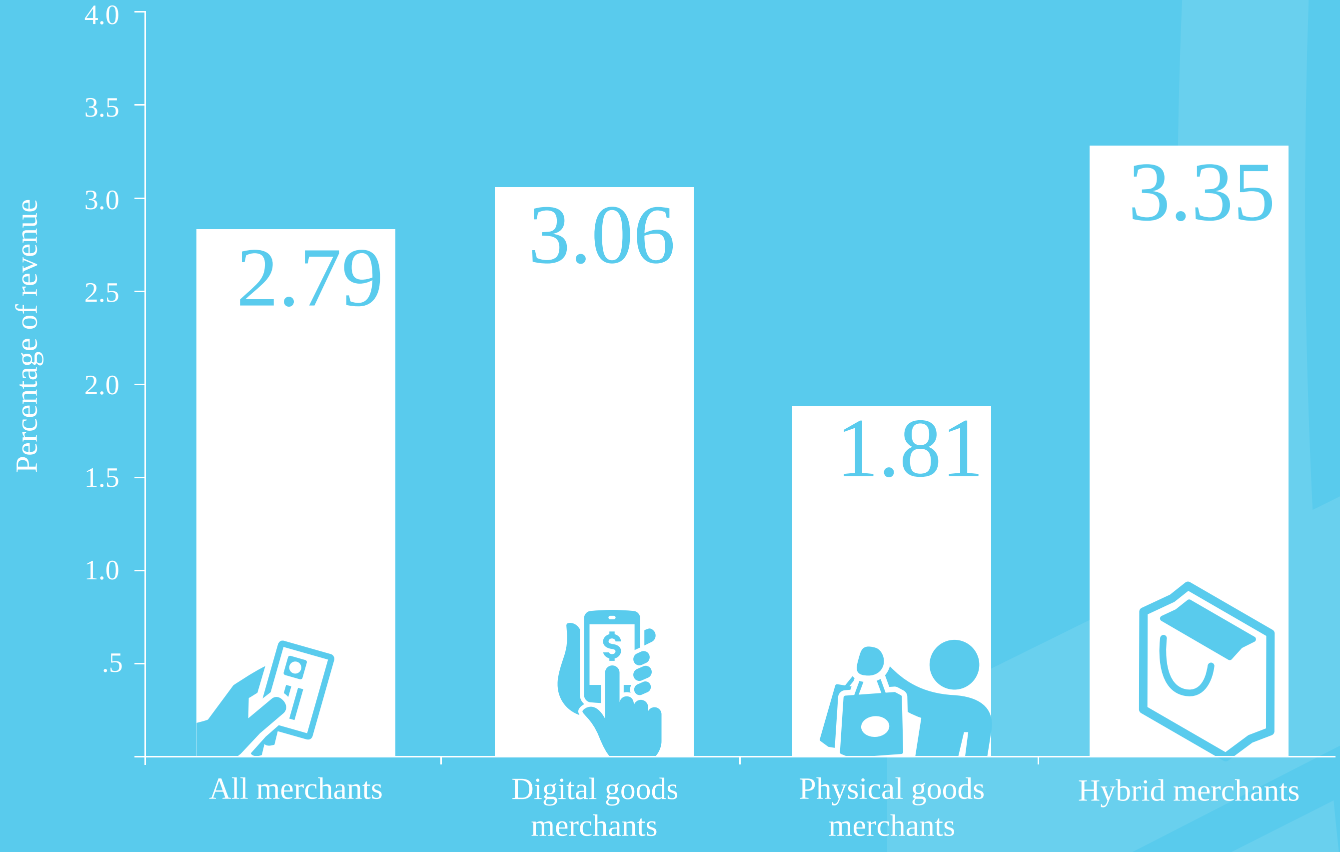
Nearly a third (30 percent) of all transactions that are declined due to suspected fraud are believed to be legitimate. Among retail sectors, digital goods merchants face the worst plight, with 34 percent of their declined transactions believed to be legitimate. Furthermore, there will be a multiplier effect from the losses to false-positive transactions, as this inconvenience undoubtedly impacts customer loyalty and the long-term value of that relationship.

This can be personally experienced when using credit cards, since 15 percent of all credit card holders had at least one transaction incorrectly declined in the past year. In 2014 alone, this represented an annual decline amount of almost $118 billion.[1] And these numbers are likely understated, as it is impossible to determine the fraud status of all declined transactions, especially if the customer gives up without making contact with the merchant.

The foundation of electronic fraud detection has long been the search for outliers – data points that don’t fit expected patterns. However, these systems too often flag outliers that can reasonably be explained by the actual course of business, such as a shipping address that doesn’t match the billing address because the customer is traveling. As one merchant executive said, “The hardest part is trying to link customers up with other activities.”

Digital content merchants are especially vulnerable to false positives because of their need to send products out the door to buyers almost instantaneously. Customers want one-click ordering, and they expect it to be secure. Merchants responding to their customers’ preferences, however, may become too lax with their anti-fraud strategies and risk losing revenue to fraudulent transactions. On the other hand, if their rules are too strict, they risk losing legitimate revenue and customers through declined transactions.

Losses From False-Positive Declines as a Percentage of Revenue



Roughly **3%** of Sales Revenue Is Lost to False Positives

VESTA

Digital content merchants are especially vulnerable to false positives because of their need to send products out the door to buyers almost instantaneously.

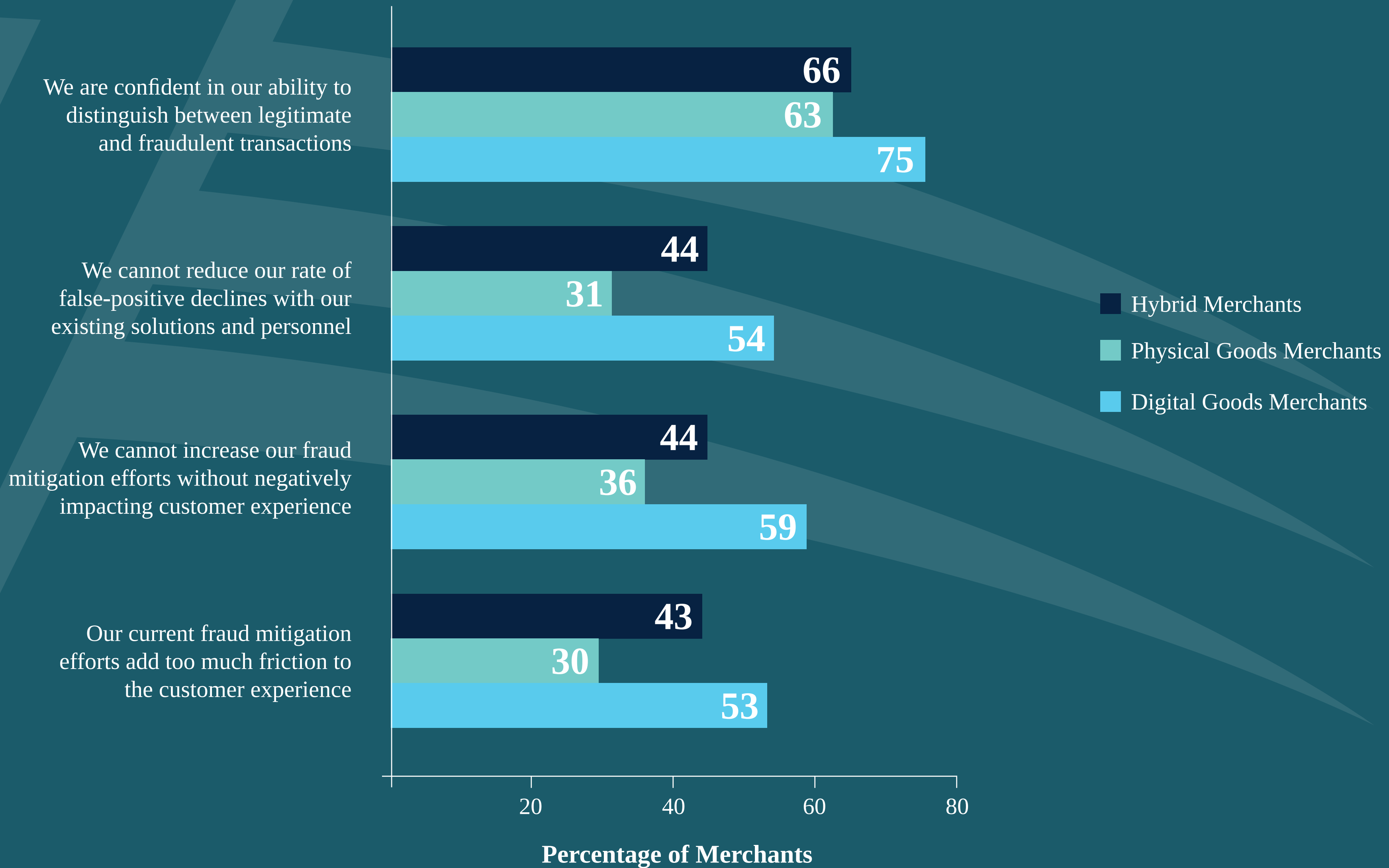
False Positives and the Customer Experience

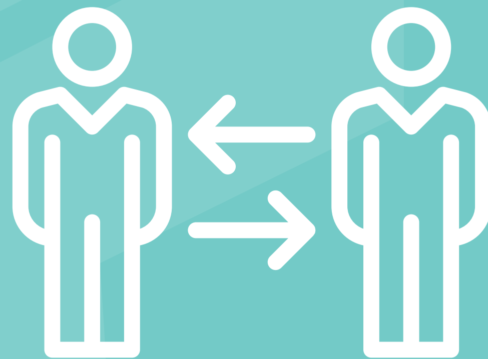
Clearly, fraud prevention can be a double-edged sword for merchant revenue, as being overly cautious or using the wrong metrics can result in sizable losses. But friction in the customer checkout experience is also a major problem.

Research has shown that when online authorization of a credit card is declined on the first attempt, most customers will try a second time. Some may even give it a third go or try with a different card if they have one. But thereafter, most will abandon the attempted purchase, often believing the site or merchant brand is to blame. And they leave with a very high risk of never returning to complete the sale.[2]

Merchants already face high losses from false-positive declines, and roughly one-third to one-half of them believe that they cannot further reduce their false-positive rates with the solutions that now exist. Digital goods merchants are the most likely to report that they are not only unable to further reduce false positives – they're also negatively impacting the customer experience as a result of their current fraud controls.

Merchants Believe They Are Controlling Fraud as Best They Can Without Affecting Customer Experience





Roughly one-third to one-half of merchants believe that they cannot further reduce their false-positive rates with the solutions that now exist.

Merchants, especially those operating online, are thus caught between two difficult choices. They face the risk of alienating a customer when they decline a sale, but they may incur losses by approving a fraudulent transaction. This means that at least for the time being, merchants will have to continue seeking the right balance between making transactions easy, quick and convenient for their customers while maintaining strong anti-fraud measures to protect their bottom lines.

To learn more about the operational costs and challenges of fraud and payments management, download **The Financial Impact of Fraud Report**

Works Cited

"The Financial Impact of Fraud." Javelin Strategy & Research, Vesta Corporation. October 2016. http://info.trustvesta.com/research2016

[1] https://www.javelinstrategy.com/coverage-area/future-proofing-card-authorization

[2] https://baymard.com/blog/credit-card-declined

VESTA

Contact Us

Americas

Vesta Corporation
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

Europe

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

Asia

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

Vesta Corporation is the only global provider of integrated fraud and payment solutions for enterprise partners in the telecom, digital goods, media and financial industries. The company's guaranteed CNP payment solutions and innovative, patented fraud technology are proven to increase conversion and acceptance while eliminating fraudulent transactions and merchant liability. Vesta holds multiple patents and has been recognized as a leading innovator in payment technologies. Founded in 1995 and headquartered in Portland, OR, Vesta's operations span the Americas, Europe and Asia.