Whitepages PRO

Five emerging eCommerce fraud threats

AND HOW TO STOP THEM

eBook

Table of Contents

Introduction

The threat of fraud is significant, persistent, and ever-changing — an unfortunate reality for online merchants trying to grow revenue. Sophisticated and organized fraudsters are patient enough to play the long game for a big score, smart enough to impersonate real customers or establish believable false identities with stolen data, and adaptable enough to change tactics as fraud management systems and practices evolve.

Did you know?

eCommerce fraud **increased** by **5.5%** from Q2 '16 - Q2 '17 [i]

Attempted fraud accounts for **43%** of monthly eCommerce transactions [ii]

Playing cat and mouse with fraudsters is not just a game for merchants, it's serious business. They must continuously juggle the need to satisfy customer expectations for quick, frictionless transactions while responding to changing threats. The operational cost is always a major concern when managing fraud.

While most eCommerce businesses use automation to identify fraud risks, 79 percent of those in North America still manually review orders. In fact, they manually review up to 25 percent of all orders on average. But 89 percent of manually reviewed transactions are eventually accepted.[1] That means merchants have the opportunity to improve their process even more to avoid unnecessarily spending time and money to review transactions from good customers.

2.17%

Fraud cost as a percent of revenue for ecommerce companies [iii]

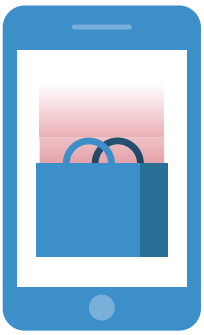
Identity verification and better automation can help. In addition to reducing fraud losses, identity verification that incorporates real-time data and analyzes the linkages between data elements can reduce the need for unnecessary manual review, prevent good customers from being rejected **(false positives)**, and help you focus on the riskiest orders.

Identity verification using real-time data, like **Whitepages Pro Identity Check**, is essential when the fraud threat is constantly evolving. In this eBook, we'll look at some of the emerging trends in eCommerce fraud and how advanced identity verification can help you meet them.

[1] CyberSource 2017 North America Online Fraud Benchmark Report, p. 6

Trend 1

Mobile commerce is booming. So is mCommerce fraud.



Consumers love their smartphones and tablets, and increasingly they love to shop with them. Nearly a third of global eCommerce purchases – which were projected to reach $2.29 trillion by the end of 2017 – were expected to be made with a mobile device,[2] up from 25 percent in 2015.[3] In some countries, notably the UK and Japan, mCommerce already accounts for more than 50 percent of all eCommerce transactions, a threshold the US has now likely passed as well.[4]

60%

of eCommerce fraud attempts originate on a mobile device [iv]

It's not surprising then that mobile devices have also become popular with fraudsters. A recent survey by CyberSource found that eCommerce retailers expect fraud losses from the mobile channel to fall just below that of their web stores, as a percentage of total revenues (.8 percent vs. .9 percent), even though mobile commerce still drives a much smaller share of overall eCommerce revenue (just 22 percent of dollars spent online in the U.S.[5]). But since 90 percent of consumers who own a mobile device consider online shopping to be a top activity[6], it's clear that retailers need to put special emphasis on identifying and stopping mCommerce fraud.

So, what can you do?

Tailor fraud strategies and practices to each transaction channel. Signals of fraud for a transaction from the desktop might not be relevant to mobile transactions. For consumers, there are special challenges when shopping with a mobile device (less reliable network connections and more data entry mistakes, for instance). Consumers also tend to shop differently when on a mobile device than they do when using a desktop. They may be less inclined to purchase high dollar items or shop for a large number of items on mobile.

Tracking customer behavior across channels and devices can provide signals that indicate unusual activity. For instance, if a customer who has only purchased small items using a mobile app suddenly purchases a large screen TV, that may be a sign that it's not a valid transaction. So the real danger in relying on the same fraud

[2] eMarketer, https://www.emarketer.com/Article/New-eMarketer-Forecast-Sees-Mobile-Driving-Retail-Ecommerce-China/1016105

[3] CyberSource, https://www.cybersource.com/content/dam/cybersource/2017_Fraud_Benchmark_Report.pdf

[4] Riskified, https://blog.riskified.com/global-ecommerce-fraud-trends-2017/

[5] Comscore, Presentation: "State of the U.S. Online Retail Economy in Q3 2017"

[6] Experian, 2108 Global Fraud and Identity Report, p. 3

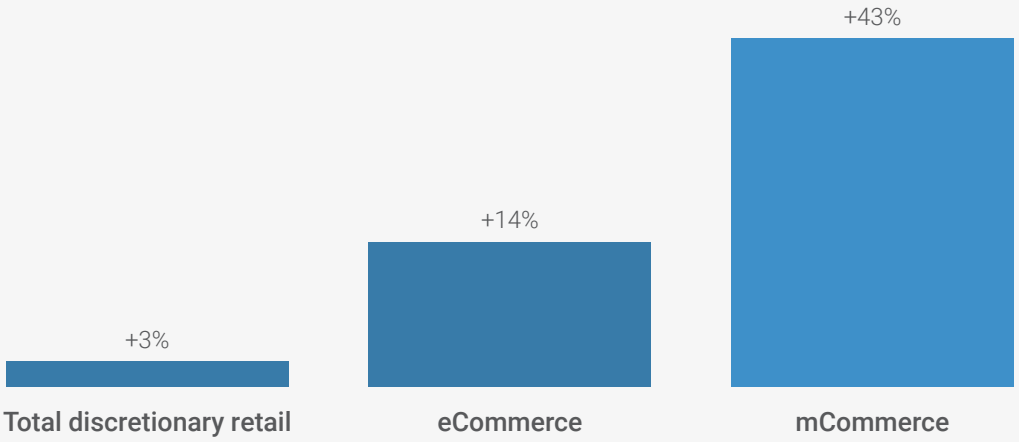
signals and applying the same practices across desktop web, mobile web, and mobile app transactions, is more false positives and increased customer insult rates.

Seems simple. But half of all eCommerce businesses (and up to 65 percent of smaller merchants) don't even track which channels are driving fraud[7], making it difficult for them to implement differentiated, channel-specific fraud strategies.

Take advantage of data that's unique to mobile transactions. For example, every mobile device has a unique device ID that can be associated with a person or previous transactions. And since consumers tend to hold on to their mobile numbers, the linkage between a person and a mobile phone number (one of the data insights provided by Whitepages Pro) is a powerful signal for verifying identity. Mobile devices are also packed with sensors that can provide a wealth of data for deeper analysis – everything from the location of the device, to the mobile carrier, to the angle at which the user holds the device. Each of these elements can be used to verify the identity of the customer and build a profile of their habits, and is even more useful when combined with other data.

In terms of discretionary spending, mCommerce growth is still far outpacing eCommerce & brick-and-mortar [v]

Q1 2017 Y/Y Retail Spending Growth by Channel



Trend 2

The upsurge in downmarket fraud

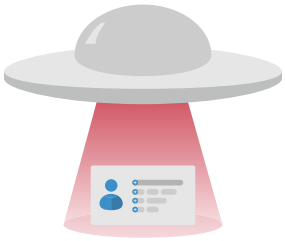
Fraudsters are not only devious, they're adaptable, changing tactics frequently in response to new fraud prevention strategies and always searching for points of least resistance. For instance, as merchants have moved to protect themselves

[7] LexisNexis, 2017 True Cost of Fraud Survey, p. 18

against fraud involving high dollar items, often adopting rules to review all transactions above a certain price point, fraudsters recently began to focus on more modestly priced items. Hitting product SKUs that usually track at very high transaction rates allows them to scale quickly.

During the 2017 holiday shopping season, for example, one Whitepages Pro customer reported a significant uptick in account takeover (ATO) fraud that targeted items like sub $300 laptops. Similarly, trendy sneakers (particularly basketball shoes) have become a hot commodity for both fashionistas and fraudsters.[8] Why? Fraudsters want items that are in demand, easy to re-sell, and fall below the radar of automatic review.

These anecdotal observations are supported by recent data. From Q1 to Q2 2017, account takeover increased by 45 percent overall to become a $3.3 billion problem for merchants. But for items costing between $100-$500 the account takeover rate rose by a staggering 151 percent[9] over the same period. Those numbers may actually go up as merchants begin to see the effects of **several large-scale data breaches last year** that revealed the personal and financial information of hundreds of millions of consumers.[10] Millennials, who have grown up sharing personal information online, are at particular risk for account takeover as fraudsters use the details they find on social media sites (such as names of pets, for instance) to guess passwords and the answers to challenge questions.



So, what can you do?

Take a holistic approach to managing fraud. No single fraud detection technology or solution will ever be enough to stop fraudsters who change tactics and targets frequently. It's vital that you use fraud prevention tools that fit your business model and threshold for risk and customer insult. Gartner* outlined their own capability framework for fraud prevention that includes: static data-based identification, rule-based risk assessment, endpoint profiling, entity relationship, behavior analytics, user interface protection, and continuous risk assessment

They point out that the capabilities are not equivalent to solution type and there is overlap, but we believe key point is that there is a move away from one-off fraud detection methods. According to Gartner, "as techniques become more sophisticated, SRM leaders are able to move beyond hindsight-based methods, which detect historic patterns of fraud, and attempt to prevent these patterns from reoccurring. The trend is toward methods that provide insight and action-oriented intelligence as to the risk of each customer interaction... Gartner observes that the

[8] https://thenextweb.com/insider/2017/02/17/sneakers-are-becoming-a-hot-online-fraud-target/

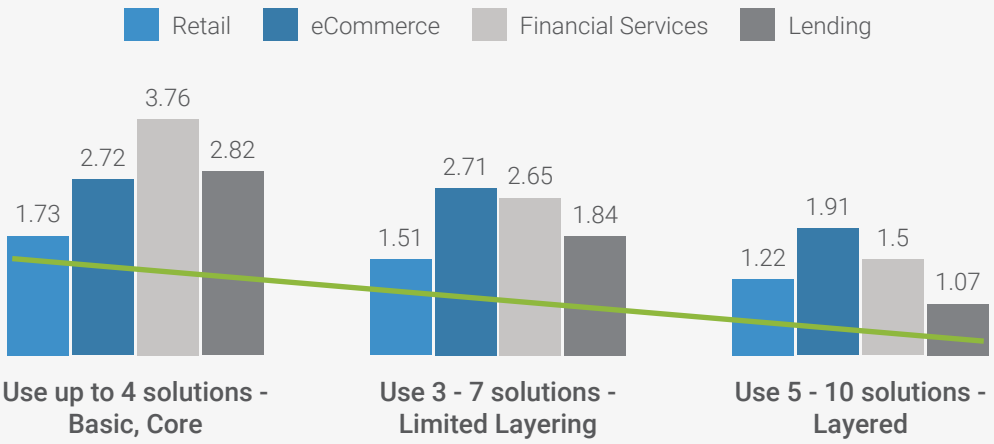
[9] Global Fraud Index October 2017

[10] https://www.crn.com/slide-shows/security/300096951/the-10-biggest-data-breaches-of-2017.htm

most successful fraud detection and prevention strategies make use of rules and machine-learning techniques in their implementations."[11]

We believe we provide solutions in the "entity relationship" capabilities, through our graph technology. Whitepages Pro Identity Check provides global real-time identity data and **proprietary network insights** to deliver an accurate indicator of risk on every transaction, the **Confidence Score**. We do this by applying pattern recognition, predictive analytics and machine learning to the five core consumer data attributes of email, phone, person, physical address, and IP to link online and offline identity attributes.

Average fraud cost as percent of revenue by number and layering of fraud mitigation solutions [vi]



Pay close attention to transaction histories and velocities. People are creatures of habit. They follow patterns in what they purchase, where they shop and how often. So if a grandmother who has historically shopped online for knitting supplies and lawn gnomes suddenly starts ordering expensive high-fashion jeans or Kyrie Irving signature basketball shoes, it may be a signal of fraud. Fraudsters also tend to try and order as much as possible from a stolen account before it can be shut down. So if a customer's orders suddenly increase in frequency or volume, that can also signal fraud. Using Whitepages Pro Identity Check, you can benefit from network insights, including multiple identity element velocities, transactional frequencies and linkage history attributes that continually identifies and adapts to these fraud patterns.

[11] Gartner, Market Guide for Online Fraud Detection Published: 31 January 2018 ID: G00318445, pg 9

Trend 3

Attack of the zombie shopping bots

Account takeover has been a persistent and growing problem for merchants, driven largely by the availability of stolen credentials and personal financial data on the dark web. But fraudsters have recently become more sophisticated in the way they exploit the trust between a merchant and customer. Rather than simply relying on stolen credentials obtained by hackers, fraudsters are going directly after consumers.

Through human engineering, phishing and/or malware attacks, fraudsters are gaining physical control of their targets' computers. A consumer who opens an email attachment that appears to be from a legitimate sender could unknowingly download malware. They may also get a social networking friend request or an email from their bank that directs them to an authentic looking, but fake website where their credentials are stolen or their machines are compromised.

Once fraudsters have gained access to a computer, they can monitor the user's browsing behavior and use malware like keyloggers to capture password information. Then they "tunnel" into the unknowing consumer's machine and use their credentials to remotely place orders from merchants. Fraudsters are even smart enough to hide order confirmations from the computer's owner by using hidden and unchecked trash folders as an alternate email inbox, allowing attacks to go on for days or even weeks.[12]

For merchants, this sort of attack is particularly troublesome because the customer's IP address, device ID, location, and other device-specific information appear to be legitimate. But fraudsters have effectively turned the consumer's computer into a shopping zombie.

So, what can you do?

Leverage a wide range of data, including biometrics in your fraud model. Relying on static data such as device ID, IP address, etc., could leave you vulnerable to shopping zombies. But even when a fraudster has control of a user's device, it may be possible to determine that it's being controlled by someone other than the customer. Using biometric information - like whether and how a customer uses a mouse or a trackpad – in the analysis can provide signals of risk (or of a good customer).

Look for divergence from previous order patterns and histories. As mentioned above, order history can be a powerful tool to identify unusual purchasing patterns

[12] https://www.avanan.com/resources/phishing-alternate-inbox

and potential fraud. If a customer is buying different kinds of items, shipping them to new locations, ordering more frequently, or shopping at unusual hours, it's possible that their machines or credentials have been compromised. This is also where identity networks can play a crucial role. With access to millions of transactions across many merchants, Whitepages Pro's Identity Network can "see" the patterns that would show up when a fraudster is placing multiple orders across many merchants in a short period of time. Combinations of order attributes, such as the email address or shipping address, can show up across the network on multiple transactions, signaling potential fraud.

Trend 4

Patient fraudsters going for the big score

While the conventional wisdom is that fraudsters want to strike quickly, steal what they can, and move on, they may be adjusting their tactics. Merchants are seeing a disturbing new trend in which fraudsters take over an account and, rather than going for a quick score right away, begin placing small and then increasingly larger orders until they eventually go for a big ticket item. They may start with items that cost less than one hundred dollars and then "graduate" to others costing thousands. This scenario can play out over weeks as the fraudsters essentially "train" the merchant to accept increasingly larger orders as genuine. With smaller ticket items possibly passing through as "good orders", it may in part account for why the fraud rate for items over $500 is 22 times higher than it is for items under $100.[13]

20%

Amount of total credit losses in 2016 due to syntehtic identity fraud [vii]

This level of patience among fraudsters is also evident in synthetic identity theft. Rather than stealing an identity, cybercriminals create a new "person" by combining real and fake information - say a child's social security number with a fake name, address and date of birth. They then use the new identity to take out credit cards or loans and use them to purchase goods. They may even pay the bills for a time to build up a credit score and increase their purchase limits. Eventually, when their credit limit reaches a certain level, they max the cards out and stop paying the bills. These sorts of scams can be months or years in the making.

[13] https://www.signifyd.com/blog/2017/10/26/new-study-reports-57-8-billion-ecommerce-fraud-losses-across-eight-major-industries/

In 2016, synthetic identity fraud led to almost $6 billion in credit losses and may account for as much as 9 percent of all credit card applications.[14] Recent data breaches are likely to make the problem even worse. While this isn't an issue that directly impacts merchants (since card issuers are responsible for the losses) it does show how far fraudsters are willing to go to play the long game for a bigger score.

So, what can you do?

Make sure to adjust your fraud rulesets regularly. Just as fraudsters change their tactics regularly, you should be reviewing your fraud rulesets on an ongoing basis to ensure they are properly configured for the current threat environment. For instance, you may need to change the parameters regarding what triggers a manual review for a returning customer based on the frequency of orders or the dollar amounts for transactions. Merchants with a more mature identity verification approach are also starting to leverage machine learning to evaluate and update rules more in real time.

Know your tolerance for risk. It's impossible to prevent fraud completely, but mitigating it is an exercise in balancing your appetite for losses, **automated** and manual reviews, and customer friction. You need to establish baselines for things like the cost of allowing a bad actor through, rejecting a good customer, manual review, and the lifetime value of a customer. With that information you can create fraud strategies that minimize risk (and respond to changing threats) without alienating good customers.

Trend 5

The reward and risk of cross-border commerce

Many eCommerce merchants are tapping into rapidly expanding markets around the world. Countries in Asia, Latin America, Eastern Europe, and the Middle East are seeing double digit increases in eCommerce[15], making them attractive targets for growth-minded merchants. At the same time, many of the fastest growing markets are also considered some of the riskiest for fraud.

As merchants have extended their reach to other countries, they've gotten better at managing fraud. In 2017, the fraud rate for international transactions (among

[14] https://www.creditcards.com/credit-card-news/fraudsters-creating-synthetic-identities-from-info-on-web.php

[15] http://www.paymentscardsandmobile.com/fastest-growing-e-commerce-markets/

Top Ten

Fastest growing eCommerce markets [viii]

1. China (64%)
2. Malaysia (47%)
3. Indonesia (45%)
4. Saudi Arabia (43%)
5. Russia (42%)
6. Argentina (38%)
7. Vietnam (37%)
8. Mexico (30%)
9. Israel (25%)
10. Hungary (24%)

North American merchants that accept international orders) reached parity with domestic transactions (.9%) down from 2x in 2012. But the rejection rate due to the suspicion of fraud was more than double that of domestic orders (6.8% vs. 2.9%).[16]

While the success of merchants in reducing the international fraud rate in recent years speaks for itself, high order rejection rates might be an indication that their fraud management strategies are too conservative — potentially turning away good customers and driving down revenue. Merchants need to strike a balance in order to maximize the opportunity presented by high growth markets without unduly increasing their exposure to fraud.

So what can you do?

Understand how identity data varies across countries and regions. One of the key challenges in managing fraud across borders is the lack of common standards for basic identity factors. Data elements that can be used to assess risk in North America, such as home address, might not work as well elsewhere. The ability to link data elements is more challenging, with maturity of each data market and privacy laws affecting use. Digital signals tend to be more global, such as email and IP, but having only a piece of the picture impacts decisions. Also, depending on the country or region the transaction is from, variations exist in which data elements are risky.

Take a holistic approach to fraud management. As described above, this approach to fraud management can be a boon not just for domestic business, but also international transactions. In particular, having a one-stop global identity data provider (such as Whitepages Pro) that enables normalization and validation for data elements (addresses, for instance) to standardize in your system, as well as deliver real-time analysis on the linkages between data elements, allows you to tailor your fraud strategies to the individual countries and regions that matter most. Not only can a holistic approach be more effective at reducing fraud, it can actually be more cost effective. For example, going from a basic to system-based approach on 5-10 solutions can reduce the cost of fraud from 2.7 percent to 1.9 percent as a percentage of revenue.[17]

[16] Cybersource, 2016 Annual Fraud Benchmark Report, p. 11 and Cybersource, 2017 North America Online Fraud Benchmark Report, p. 9

[17] http://images.solutions.lexisnexis.com/Web/LexisNexis/%7B44c6207d-7c96-40e7-aa85-a3cc17483139%7D_LexisNexis_Risk_Solutions_2017_True_Cost_of_Fraud_Study_--_Overall_Report.pdf, p. 38

Conclusion: What's next?

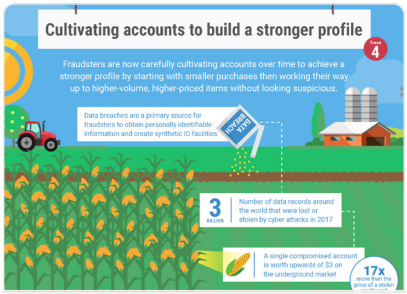
The only thing that's constant in the fight against fraud is that it's always changing. These trends are just the latest fronts in an ever changing and never ending battle.

It's easy to predict that certain trends are likely to continue and even accelerate. Account takeover, for instance, shows no signs of slowing down and may even pick up as fraudsters take advantage of the flood of personal information exposed in the highly publicized major data breaches of 2017. Similarly, as consumers continue to shift their online time to mobile devices and more merchants offer mobile-optimized shopping experiences, the percentage of eCommerce transacted via the desktop will continue to fall. Some trends may also fade away. As merchants respond to threats, such as down-market fraud attacks, by **adjusting their fraud strategies and rulesets**, fraudsters will inevitably look for another weak link to attack.

Looking ahead, emerging technologies such as consumer Internet of Things (IoT) devices, and voice-enabled assistants will inevitably provide fraudsters with more new vectors to exploit. Merchants will have another risk factor to consider: How to assess the identity and fraud risk from an Internet connected refrigerator that a consumer has authorized to automatically purchase groceries?

Regardless of what the future holds, merchants need to have real-time global customer identity data, linkages, and network insights that can be incorporated into their fraud management platforms and decisioning systems. Whitepages Pro Identity Check offers access to the most comprehensive global consumer data, insights from millions of transactions from our Identity Network, as well as **valuable tools like our Confidence Score**, to prevent fraud and improve customer approvals.

If you'd like to learn more or speak with a Whitepages representative, **click here.**



INFOGRAPHIC

Five eCommerce Fraud Trends on the Rise

Download infographic

EBOOK

Grow Cross-border eCommerce and Mitigate Fraud

Read the eBook

DATA SHEET

Identity Check Risk Indicators for eCommerce

Learn more

Additional sources

[i] ***Total fraud increased by 5.5% from Q2 2016-Q2 2017***

Source: Global Fraud Index (PYMNTS.com and Signifyd), https://www.pymnts.com/global-fraud-index/

[ii] ***Attempted fraud accounts for 43% of monthly eCommerce transactions***

Source: LexisNexis - 2017 True Cost of Fraud Study, p. 8, https://risk.lexisnexis.com/insights-resources/research/2017-tcof

[iii] ***2.17% fraud cost as a percent of total revenue for eCommerce companie***

Source: LexisNexis - 2017 True Cost of Fraud Study, p. 14, https://risk.lexisnexis.com/insights-resources/research/2017-tcof

[iv] ***60% of eCommerce fraud originates on a mobile device***

Source: RSA, https://www.pymnts.com/news/security-and-risk/2017/fraud-account-takeover/

[v] ***mCommerce growth***

Source: Comscore, Tech Savvy Shoppers are Transforming Retail

[vi] ***Fraud cost as a percent of revenue by number & layering of fraud solutions***

Source: LexisNexis - 2017 True Cost of Fraud Study, p. 38, https://risk.lexisnexis.com/insights-resources/research/2017-tcof

[vii] ***20% of total credit losses in 2016 due to synthetic identity fraud***

Source: Auriemma Consulting Group, http://www.acg.net/synthetic-identity-fraud-cost-banks-6-billion-in-2016-auriemma-consulting-group/

[viii] ***Top Ten Fastest Growing eCommerce markets***

Source: http://www.paymentscardsandmobile.com/fastest-growing-e-commerce-markets/

[*] ***Note:***