2019
SIXTH ANNUAL

Fraud Attack Index

FORTER®

Introduction

Today's e-commerce payments ecosystem is dynamic. With more users online than ever before, and retailers expanding beyond their brick and mortar stores and e-commerce platforms to bridge the gap with omni-channel offerings, the retail world is growing.

As the means by which customers shop change, so too do the avenues fraudsters navigate in order to commit online payment fraud. Fraud techniques are ever-evolving, and online criminals are growing more sophisticated in their methods and capabilities. **Instead of launching one-off attacks, they are turning more often to automation**, leveraging bot attacks at scale and collaborating with other fraudsters to create powerful fraud rings with a breadth of knowledge.

Online retailers must understand the world of online fraud in order to protect their businesses. Opportunistic fraudsters are looking to diminish their bottom line and pollute their customer ecosystem. An understanding of payment trends in the market, combined with insights into how fraudsters approach and attempt to commit online fraud, will arm retailers with the ability to ensure that their businesses and their customers are protected from the most common fraud methods and vulnerabilities.

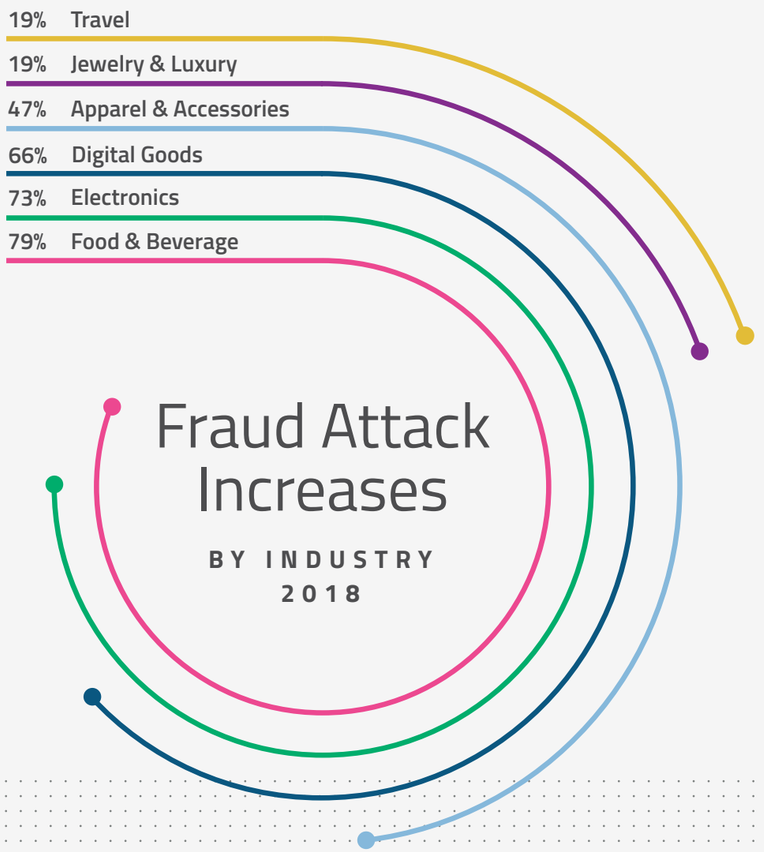
> "Fraud techniques are ever-evolving, and online criminals are growing more sophisticated in their methods and capabilities.

1
About This Report

Forter's biannual Fraud Attack Index highlights the rapidly shifting e-commerce landscape and breaks down how changes in this fragile ecosystem can affect online merchants and their omni-channel offerings. The report leverages Forter's data to examine the trends in online fraud attacks across industries, exploring the fraudulent modus operandi (MO) or methods fraudsters may use to attack online retail platforms.

Criminal access to personal data online has never been richer, partially due to recent data breaches, but also in part because of the expanding nature of ambitious fraudsters and the growing need for individuals to meld their online profiles with their real-life identities. **Fraudsters have access to more private information than ever before**, and as online criminal networks expand, the access to phishing kits or "crime-as-a-service" opportunities increase for new fraudsters, lowering the bar for more users to enter the ring.

This report analyzes fraud attack rates, rather than successful fraud, in order to explore current fraud patterns along a variety of industries, and help merchants better understand attacks they may already be seeing and prepare for ones that they are likely to encounter.



2 Industry Breakdown

INDUSTRY BREAKDOWN

Food & Beverage

79% increase

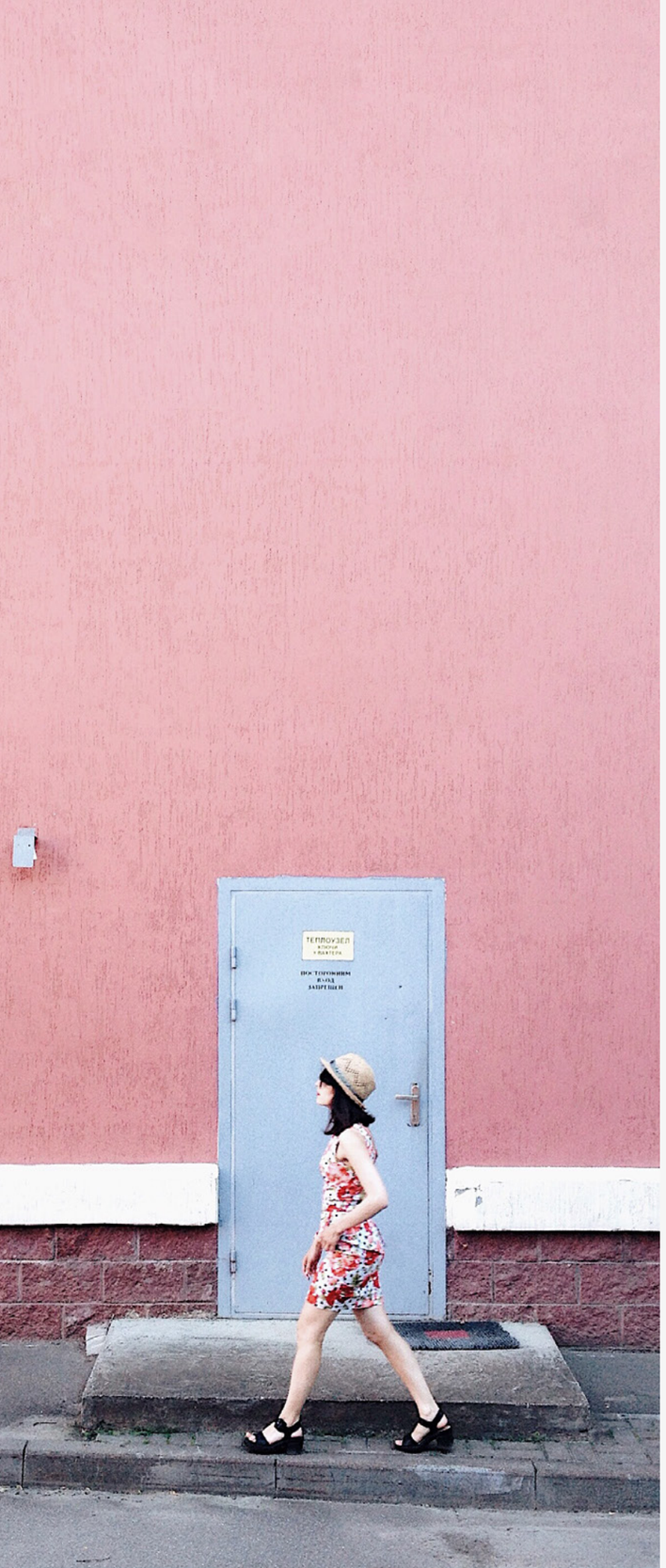
Attacks against online food and beverage businesses (including restaurants, delivery services and merchants in this industry) **have shown an increase in fraud for the second year in a row.** 2017 saw an increase of 60%, and comparing the Q4 2017 numbers to Q4 2018 shows an increase of 79%, indicating that this sector has retained and if anything increased its appeal to fraudsters.

There are numerous examples of fraudsters stealing for their own direct benefit rather than for monetization, especially with resellable items like high-end alcohol. In general, the popularity of this industry with criminals is due to its use as a payment testing zone — fraudsters testing out cards or wallets to see if they can get away with the purchase. Once successful, they know it is worth trying for a higher ticket order elsewhere.

INDUSTRY BREAKDOWN

Apparel & Accessories

47%
increase



Attacks on online apparel saw an increase over 2017, and unfortunately that trend has continued over 2018. Comparing the Q4 results of each year shows a 47% increase in 2018. **Apparel remains popular with fraudsters because it is easy to resell, and attempts to buy in bulk are not suspicious as is the case in many other industries.** Good customers often buy apparel or accessories for groups or teams, or purchase items in more than one color or material. Legitimate buyers are frequently willing to make purchases from third party sites, making reselling much easier. The result is that fraudsters in this industry can feel confident of a good ROI.

SPOTLIGHT

Limited Edition Footwear

One of the challenges that has developed in this industry over the last year is how to combat BOTs (automated scripts which can run specific actions over and over again with great speed). In this industry, BOTs are used to target new releases of limited edition items. Such specialty items are often popular in the criminal community as their rarity gives them extra value and ensures an eager market. However, fraudsters are not the only ones using BOTs in the apparel industry; as has been seen in the sneaker scene, collectors and resellers are getting in on the BOT action as well.

INDUSTRY BREAKDOWN

Jewelry & Luxury

19%
increase

Jewelry and luxury have always been attractive for criminals due to their high value. This means that even a single successful theft can be very lucrative. Since the overwhelming majority of fraudsters are in it for the money, and many even organize their theft more or less as a business, jewelry and luxury goods emerge as natural targets. Merchants in this sector are aware of the high risk they run with their products, and take appropriate steps to avoid the danger. Nonetheless, the appeal of these goods means that fraudsters keep trying. In 2018, looking at a Q4 2017 to Q4 2018 comparison, attacks rose 19%. This demonstrates the evergreen draw of these pricey items with fraudsters looking to make a quick buck.

INDUSTRY BREAKDOWN

Travel

Air travel has seen a decrease in fraud attacks over 2018, showing a dip of 29%. This indicates that the large data hacks within the industry, some of which made passport information available along with other stolen data, have yet to be reused to commit air travel fraud. This data is valuable enough to be leveraged for fully fledged identity theft (which may have many stages) rather than “thrown away” on a single fraud attempt. **Within this industry, it is notable that there is a difference between the fraud attack rates seen by major airlines and by low cost airlines, with major airlines attacked 37% more.**

Land travel and accommodation, on the other hand, witnessed a 19% increase in attack rates. As hotels, car rentals and train services aim to optimize for customer experience, they face challenges when it comes to fraud prevention. An ideal customer experience means removing some of the traditional barriers like requiring proof of identity. This provides fraudsters with an opportunity. Transactions and bookings where the payment is made online in advance are particularly prone to attack, but are also increasingly popular with good customers. This industry will need to be especially careful to emphasize accuracy in antifraud going forward, avoiding risk-averse approaches that often result in false positives while also minimizing fraud.

Digital Goods

Comparing the numbers from Q4 2017 to Q4 2018 shows a decrease of 27% in fraud attacks against digital goods, but this can be accounted for by the fact that Q4 2017 saw a sharp spike that evened out the following year. Comparing the Q3 results of the same years shows an increase of 66%, showing that in digital goods considerable fluctuation in attack rate is still normal.

Overall, the attack trends against digital goods in 2018 showed that the industry remains consistently appealing to fraudsters. This is unsurprising, as digital goods has a number of elements that make it an ideal fraud target. As customers receive their purchase in close to real-time, fraudsters do not need to fear losing their goods if a charge-back occurs shortly afterward. Additionally fraudsters dodge the need to include a shipping address, which can be a challenge with physical goods. Criminals can monetize digital goods easily, quickly and at scale. As such it is likely that digital goods will continue to be fraudster favorites for the foreseeable future.

> "Criminals can monetize digital goods easily, quickly and at scale.

INDUSTRY BREAKDOWN

Electronic Goods

73% increase

The electronics sector has seen consistent popularity throughout 2018, and comparing Q1 2017 to Q1 2018 shows an increase of 73%. During 2018 the attack numbers remained high with only minor fluctuation. The decline of 5% seen by comparing Q4 2017 to Q4 2018 should be seen within this context; the small dip falls within standard fluctuation and is little enough not to indicate a pattern, particularly against the background of a strong trend of attack interest.

> Electronics remain appealing to fraudsters given their value and the ease with which they can be resold.

Electronics remain appealing to fraudsters given their value and the ease with which they can be resold. Customers are used to buying from third party sites to get better deals, and fraudsters can market their stolen items as “refurbished” to explain a discounted price and make the sale even more likely. Moreover, as good customers often buy multiple electronic items at once (for example, a laptop plus keyboard and mouse) fraudsters are more likely to get away with a good haul.

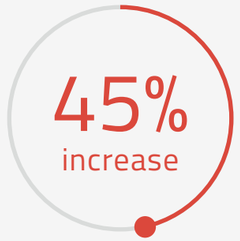
3 Methods of Attack

THE CUSTOMER JOURNEY

Merchants need to protect their platforms beyond just the point of transaction. For years, legacy fraud systems and rules-based solutions have focused on the point of sale, neglecting the larger picture and the vulnerabilities before a customer makes it through to checkout.

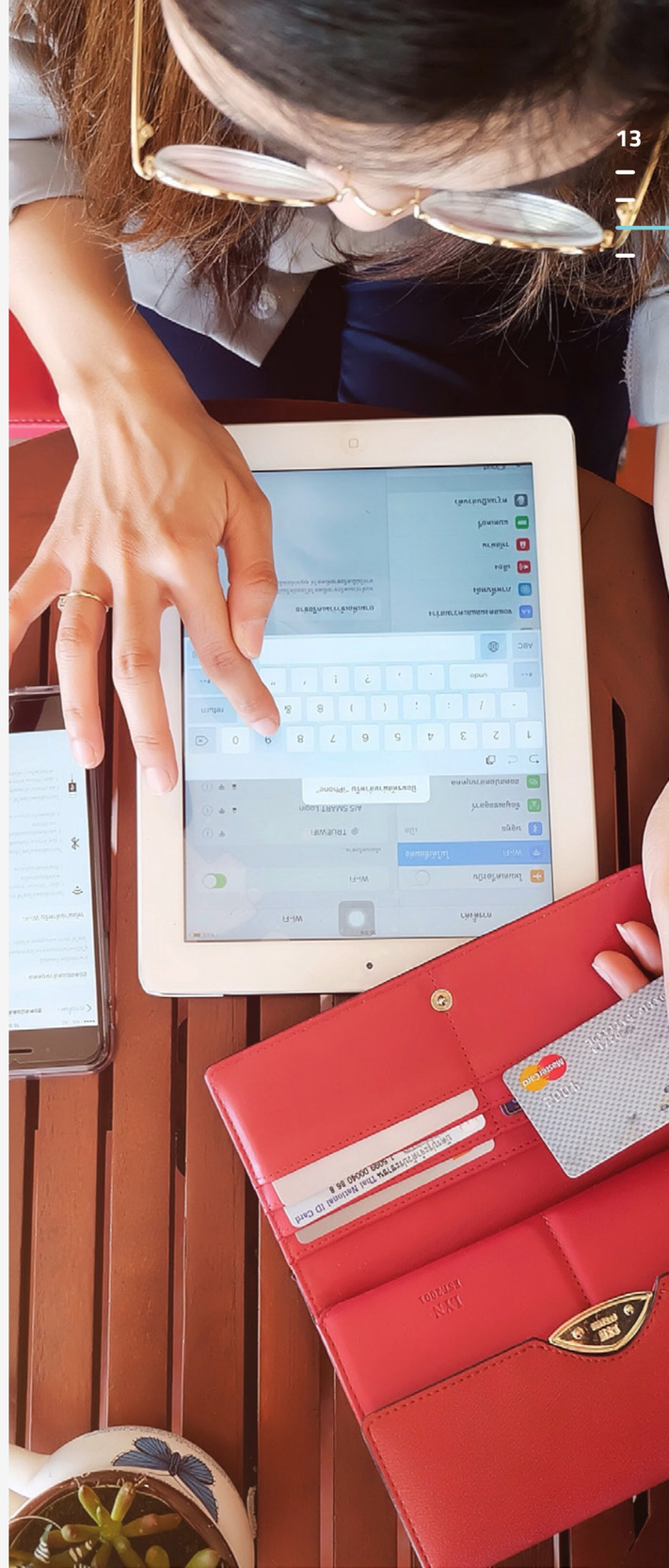
Protecting the customer journey means understanding each of the touch points and interactions a shopper may experience prior to the point of transaction. This ranges from the moment a customer navigates to a merchant's site to the point at which they log into their account or try to redeem any reward points they may have. Merchants need an "always on" solution. Retailers and fraud prevention professionals will have to adopt a more nuanced understanding and holistic view of their customers' shopping experience to understand how to protect them from end to end.

Account Takeover



Account Takeover (ATO) occurs when a fraudster gains unlawful access to an account in order to exploit it. ATO fraud has proven useful to online criminals who have realized that stealing a user's account offers more opportunities than typical transactional fraud. Through ATO, fraudsters can hack into accounts and add new (stolen) financials which are then used to make purchases. They can also gain access to a user's loyalty or reward points on a particular merchant's site and leverage these to make purchases, often avoiding detection from the platform's fraud monitoring. Customers are much less likely to review their loyalty points usage or accrual as they would their normal bank or credit card statements. ATO fraudsters demonstrate a pattern of using the easiest and least noticeable payment methods available first (gift cards, rebates, and store credit) and only if those are used or unavailable, card or wallet.

ATO spiked at the beginning of 2018, perhaps reflecting the fact that a number of the large scale breaches of 2018 included payment data. When this is the case, such information is typically used for fraud directly rather than leveraged for ATO attacks. Generally speaking, ATO has remained high, increasing by 45% by the end of 2018 compared to the beginning of 2017.



METHODS OF ATTACK

Fraud Rings

An increasingly common phenomenon has been the rise of fraud rings. This occurs when online criminals band together to collaboratively commit fraud. In this manner, fraudsters are able to leverage the skills and expertise of individual fraudsters and form highly specialized fraud rings that are difficult to identify and stop. Forter has seen that the returning individual offender rate has decreased in response to the rise of fraud rings, which have grown by 26% this year.

Fraud rings will continue to grow in the coming year, as fraudsters understand that by working together they can do more damage.

Fraud rings can collaboratively pinpoint specific vulnerabilities in the customer shopping journey and leverage the very best fraudsters to exploit each of these touch points. They are able to leverage bots in order to scale their attacks so they can both tailor their methods and strike at a higher frequency, wreaking havoc on e-commerce merchants.

SPOTLIGHT

Coordinating Sophisticated Fraud

Fraud rings are highly sophisticated - these criminals band together and leverage the expertise of members of the group in order to execute seamless attacks, avoiding merchant and potential victim detection. Typically, fraudsters will gather personally identifiable information (PII), either collected from recent data breaches, or via phishing campaigns run by the fraud rings themselves. Using bot attacks they then attempt automated mass logins (also known as volumetric attacks), and then attempt to make transactions within accounts that they have successfully logged into. With fraud rings, an operation can carry out all stages of the attack simultaneously once they are up and running, with each criminal focusing on the stage in which they are experts. This gives fraudsters the ability to scale quickly and strike before merchant sites or victims of such attacks have even realized that they may have been exploited.

METHODS OF ATTACK

Policy Abuse

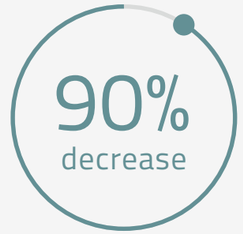
170%
increase

Policy abuse (also sometimes referred to as compliance abuse) is the method ascribed to individuals cheating merchants through use of coupons and discount codes, overusing refer-a-friend reward programs, or creating multiple accounts.

Last year Forter saw more than 200K policy abusers. This number continues to rise as Forter witnessed a 170% increase since Q4 2017. This type of abuse is often less top of mind for retailers, as they tend to focus more on transactional fraud where losses are potentially greater.

However, retailers should keep in mind that policy abuse as a growing trend can and will impact their bottom line. The oversharing of coupon or discount codes, or the creation of multiple accounts per user, will ultimately result in the contamination of a brand's customer ecosystem. As retailers become more cognizant of these types of interactions on their platform, they should bear in mind that creating system rules or stringent policy measures (aimed to protect their business) may capture potentially good customers rather than just those who intended to abuse the system.

Returns Abuse



A popular account level abuse is returns abuse, where abusers try to cash in on the looser returns policies that retailers offer. However, retailers now understand that this is a weak spot in their platform, and several large merchants, including L.L.Bean, Nordstrom, and Amazon, have amended their policies to restrict the number of returns for their customers.

As such, returns abuse has decreased by 90% compared to the Q4 2017 spike, indicating that the stricter policies many merchants have started to enforce in self-defense are starting to have an impact. **Retailers walk a fine line here – too restrictive and the return policies could have unintended consequences, turning away valued customers who are trying to return goods or products legitimately.** These good customers will then experience added friction in their shopping journey, thereby diminishing their likelihood of remaining brand loyal.

While it is vitally important that retailers take returns abuse seriously, it is even more important that they truly understand the nuances of their customers' activities to differentiate good behavior from abusive, and avoid turning away good users.

> "The stricter policies many merchants have started to enforce in self-defense are starting to have an impact.

METHODS OF ATTACK

Instrument Manipulation

13%
increase

Instrument manipulation is on the rise. As mobile devices and hardware become increasingly cheap to procure, fraudsters are turning toward this method of fraud more often. Instrument manipulation can include the use of burner phones, virtual machines, bots, remote desktop protocol (RDP), and more. Fraudsters often try to hide their activities behind these devices, flying under the radar of detection for most legacy fraud prevention systems, which are simply not equipped with sophisticated enough technology to pick up on the nuances of these behavioral indicators and the personas hiding behind them.

Forter noted an increase of 13%, reflecting the abundance of cheap, easy-to-obtain hardware. This has to some extent replaced identity manipulation wherein fraudsters use credentials (e.g. e-mail) stolen from a 3rd party to conceal themselves. However, both techniques remain popular.

4
Methodology

Our approach to data pulls involves two different measurements in order to look for patterns in the data and to best calculate fraud averages:

1

By weighting every transaction identically, where larger merchants have a larger impact on the resulting data.

$$\frac{\sum_{i=1}^{M} F_i}{\sum_{i=1}^{M} N_i}$$

Where F_i is the number of fraud transactions for merchant i and N_i is the number of transactions for merchant i and M is the number of merchants.

2

By weighting every merchants' rates and averaging those rates, so that all merchants will have equal impact on the resulting data.

$$\left\langle \frac{F_i}{N_i} \right\rangle$$

Where F_i is the number of fraud transactions for merchant i and N_i is the number of transactions for merchant i and M is the number of merchants.

The first methodology described will allow for data that is more representative towards specific merchants and therefore, may be much more dependent on specific phenomenon due to specific merchants.

The latter methodology tends to have more fluctuations due to the fact that denominators are lower.

About FORTER®

Forter is the leading e-commerce fraud prevention company that protects merchants during each stage of the customer lifecycle. The company's identity-based fraud prevention solution provides instant approve/decline decisions for every transaction and detects instances of fraud beyond the point of transaction in real time, such as during attempts at account takeover and return abuse. A team of world-class analysts constantly researches new fraud trends and updates Forter's machine learning solutions with cutting-edge insights, ensuring the proprietary algorithms adapt to the latest fraud strategies in real time. As a result, Forter is trusted by Fortune 100 companies, online travel businesses, and fast-growing digital disruptors to deliver exceptional accuracy, a smoother user experience, and elevated sales at a much lower cost.

Visit www.forter.com