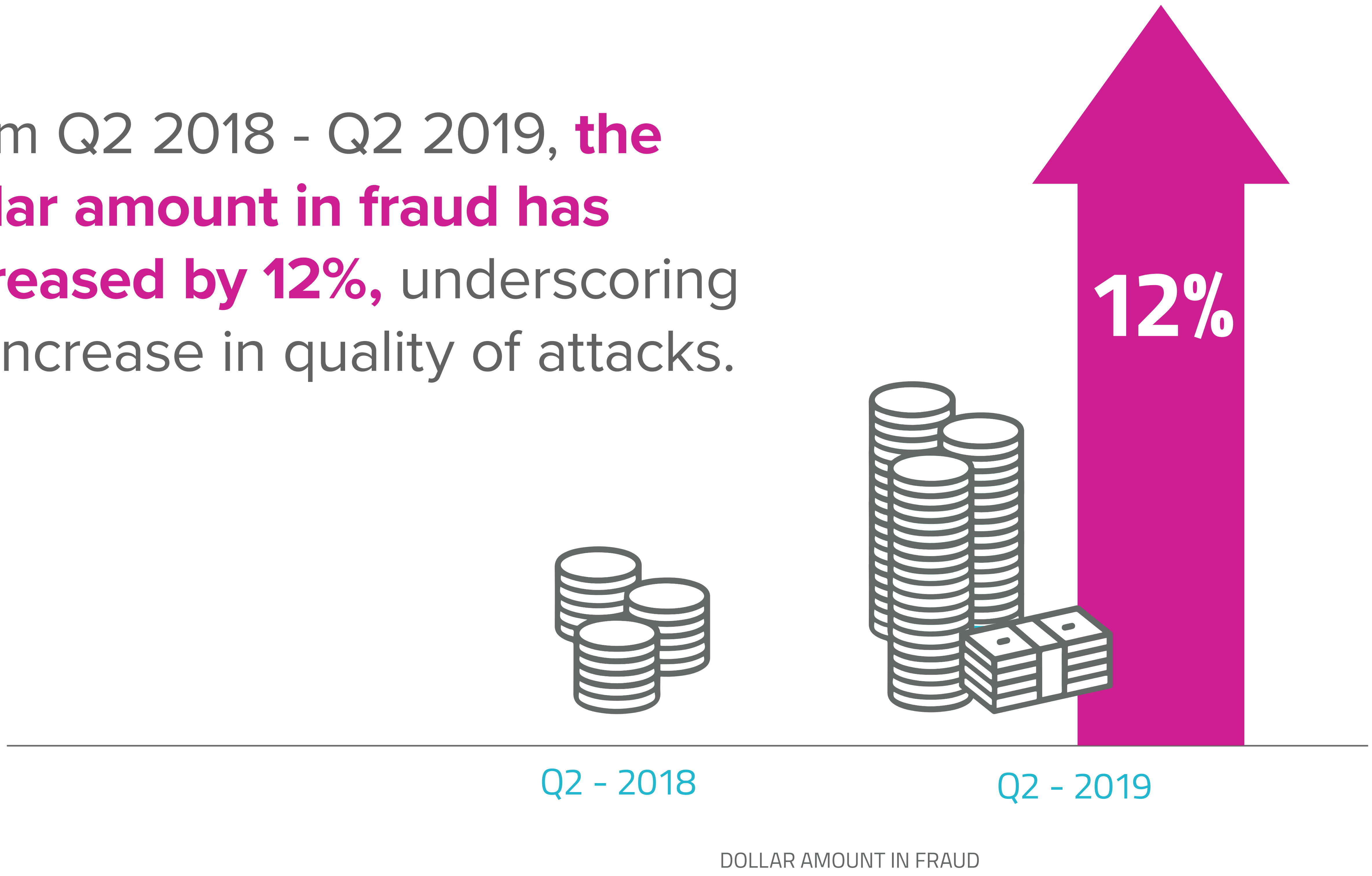
FORTER®

2019
SEVENTH EDITION

FRAUD **ATTACK** INDEX

From Q2 2018 - Q2 2019, **the dollar amount in fraud has increased by 12%,** underscoring an increase in quality of attacks.



Executive Summary

Today's payments ecosystem is shifting. Where once customers engaged only through brick and mortar stores or online via their desktops — the entirety of the customer experience has now evolved into an omnichannel one, wherein no borders exist between how consumers engage with their brands and merchant platforms.

Online retail is changing too. Connected experiences (via mobile, desktop, and in-store) are now orchestrated to work together, offering consumers the best experience no matter how or where they shop. The retail world is expanding globally, with more users and forms of engagement available along the customer journey, than ever before. Likewise, customer expectations are expanding — the new norm requires instant gratification, immediate fulfillment, and increasingly more personalization in offerings than in years past.

As the global payment and e-commerce systems shift, and the means by which customers engage with brands and products evolve, online criminals are similarly transforming how they interfere and exploit online systems. The increasing level of sophistication in attacks and fraud methods comes at a time when user experience is key. Customers now, more than ever, expect a friction-free shopping experience with no delays along their path to purchase or fulfillment. With new methods of fraud circumventing legacy fraud prevention systems, customers who meet added friction have more options than ever before and will drop off retailer sites in search of better experiences elsewhere for the same products. In a recent Forter survey, half of Americans agree that they were less likely to buy something online if the entire checkout process takes longer than half a minute. Furthermore, the average customer will wait just ten seconds for their credit card to be verified, and one in three have clicked out of purchasing their item when having to re-enter their credit card info.

As such, it is essential that online retailers understand the world of online fraud and how to better protect their businesses and bottom line from opportunistic fraudsters. An understanding of payment trends as well as account fraud and abuses in the market, combined with insights into how fraudsters approach and attempt to commit online fraud, will arm retailers with the ability to ensure their businesses and their customers are protected from the most common fraud methods and vulnerabilities.

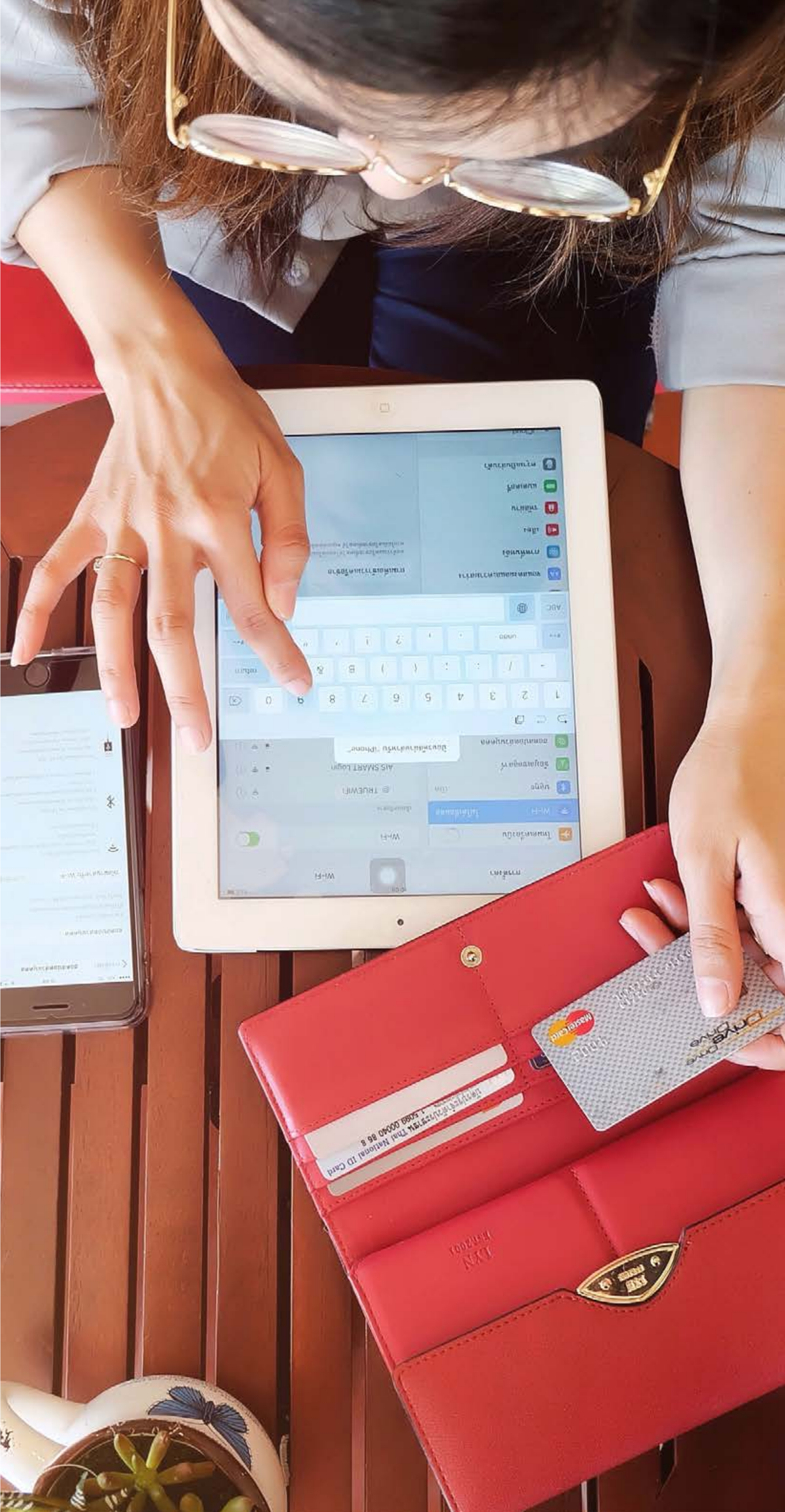


Table of Contents

EXECUTIVE SUMMARY 3

ABOUT THIS REPORT 5

INDUSTRY BREAKDOWN 6

THE CUSTOMER EXPERIENCE 19

METHODS OF ATTACK 23

FRAUD AROUND THE WORLD 33

GROWING MARKETS, GROWING YOUR BUSINESS 36

FINANCIAL INCLUSION IN A MODERN AGE 36

METHODOLOGY 37

About this Report

The Seventh Edition of Forter's Fraud Attack Index highlights changes within and across the dynamic world of online commerce. This report leverages Forter's robust database to examine shifting behaviors and trends in online fraud attacks across global industries and explores the fraudulent modus operandi (MO) or methods by which fraudsters leverage their attacks. With over $140 billion in e-commerce transactions, the Seventh Edition Forter Fraud Attack Index encapsulates the most extensive research ever conducted in this field.

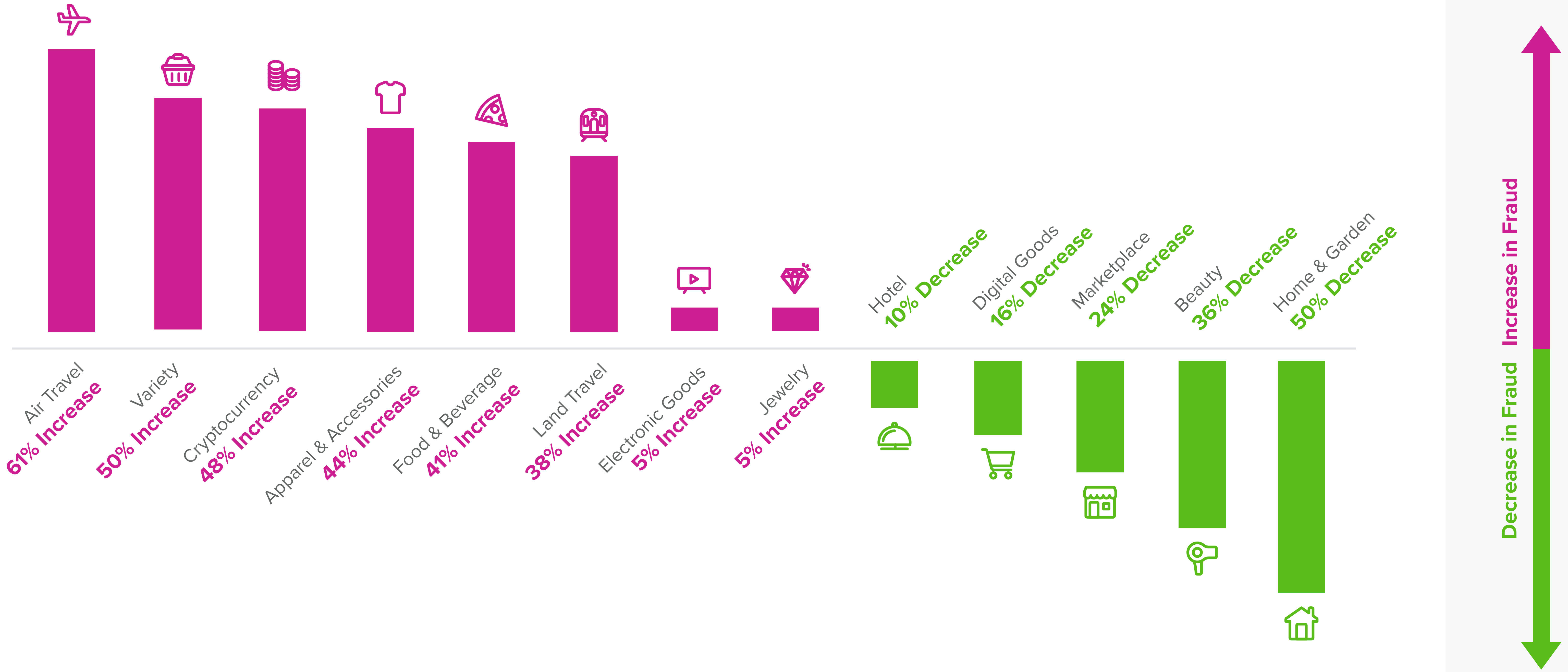
Online fraudsters are ramping up the level of sophistication of their attacks. They are shifting their focus from brute force attacks, where quantity of attacks meant the likelihood of a payoff, to investing in higher quality, targeted attacks, where one attack translates to a larger and more meaningful payoff. In part due to the data breaches of recent years, fraudsters also continue to have a wealth of personal data at their disposal and have focused their attention on account-based vulnerabilities rather than traditional transactional fraud. Fraudsters are similarly benefiting from the expected customer norm of a seamless shopping experience. By streamlining particular processes (including shipping and checkout) in order to better compete with other online brands, retailers have simultaneously created vulnerabilities in their platforms that fraudsters are looking to exploit.

This report reveals fraud attack rates, rather than successful fraud. The data reported exposes current fraud patterns along a variety of industries, in an effort to help merchants better understand the current e-commerce climate, the methods by which fraudsters are attacking, and to help businesses prepare for fraud and forms of abuse they may be likely to encounter in the coming months and year.

With over $140 billion in e-commerce transactions, the Seventh Edition Forter Fraud Attack Index encapsulates the most extensive research ever conducted in this field.

Industry Breakdown

Industry Breakdown At A Glance



44%

INCREASE IN FRAUD ATTACKS

Apparel & Accessories

Fraud attacks on the online apparel and accessories industry saw an **increase of 44% YoY**. This industry is favored by online fraudsters, since fashion merchandise is continually in high demand, the products are particularly easy to resell. Fraudsters are able to buy the merchandise and turn a profit by reselling the items for near retail price to fastidious bargain hunters. The apparel and accessories industry is also a perpetual target for fraud, since buying items in bulk, whether for sports teams or other organizations, is quite common and unlikely to raise suspicions as it might in many other industries.

36%

DECREASE IN FRAUD ATTACKS

Beauty

The beauty industry has seen an exponential rise in online activity over the last year. As more businesses turn from brick and mortar offerings alone and shift to more online channels to sell their products, the market has grown significantly. With more beauty products being sold online (think Kardashians), the denominator has grown and as such, fraud attacks have decreased. The industry saw a **36% decrease** this year, and as the market continues to grow more saturated, this phenomenon is likely to persist.

Digital Goods

Digital goods are commonly favored by fraudsters and represent in fact, the industry in which we see the best fraudsters, since digital goods are the easiest to cash out without any great efforts. This industry saw a **slight decrease by 16%** in fraud attacks. The smaller decrease in comparison to last year coincides with a broader trend that has appeared across e-commerce in general — *quality of attacks versus quantity of attacks.* Fraudsters are shifting from high rates of indiscriminate attacks to more targeted and sophisticated efforts that yield the best results.

> …quality of attacks versus quantity of attacks. Fraudsters are shifting from high rates of indiscriminate attacks to more targeted and sophisticated efforts that yield the best results.

16%

DECREASE IN FRAUD ATTACKS

Money Services & Cryptocurrency

Money services and crypto is a growing industry and an attractive target for fraudsters. There has been a **48% increase** in fraud attacks against this industry, and data indicates that this sector boasts a new playing field for up and coming sophisticated fraud schemes. Money services and crypto is a relatively new category that is rapidly growing. Whereas fraudsters will exploit the digital goods industry — specifically gift cards — given the ease of cashing out, they find an even less complicated process to monetization in the money services industry. Fraudsters here can skip the step necessary to monetize, since they're able to simply cash out immediately on financial transactions. This industry is seeing more sophisticated methods of attack, including social engineering, to capitalize on the quick path to cash.

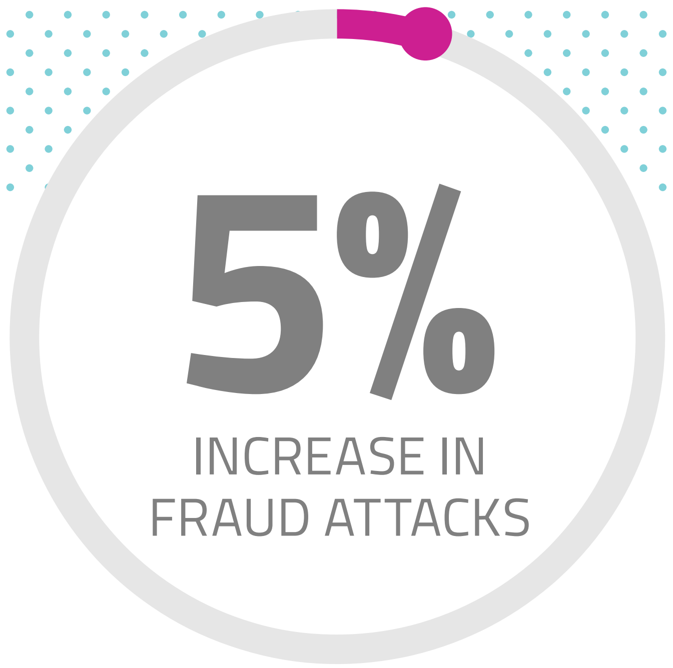
SPOTLIGHT

The Rising Investment of Fraudsters

The cryptocurrency market holds some unique traits given its volatility and the difficulty of tracing crypto transfers. These specific characteristics make this area of digital commerce a prime target for fraudsters. To avoid overhead costs, the added complexity of stealing credit cards, and the use of technological means to mask themselves to appear more like their victim, many fraudsters have resorted to contacting and manipulating their victims. In some cases, fraudsters actually reach out and contact the victims — usually less tech-savvy and older individuals — by phone or e-mail and convince them to purchase cryptocurrency with their own money and transfer it to the fraudster's digital wallet in exchange for the promise of huge returns to the victim.

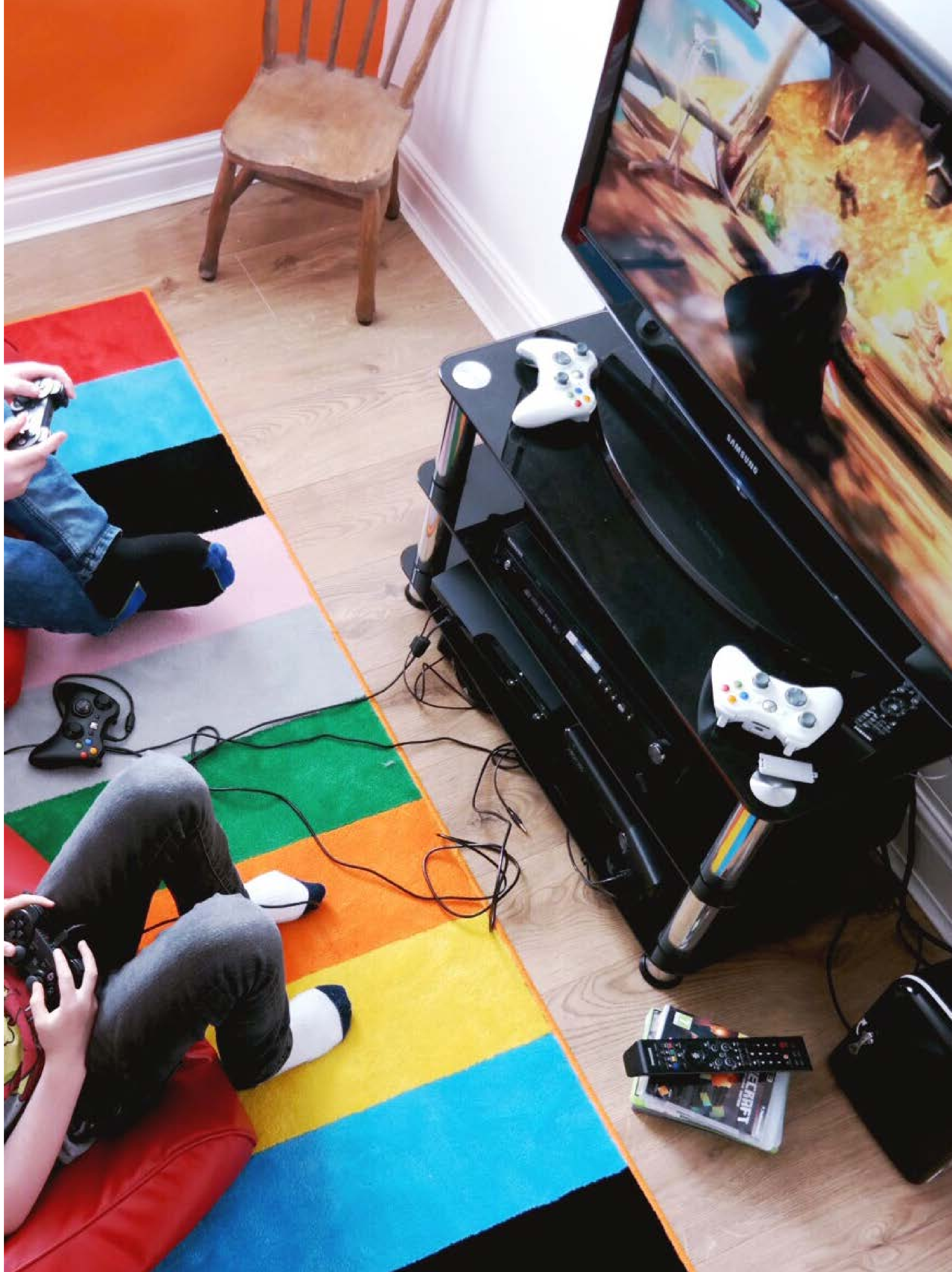
48%

INCREASE IN FRAUD ATTACKS



Electronic Goods

This year the electronics industry showed no real change. Balanced by the per merchant models, there was a **5% increase** in fraud attacks against this industry. Electronic goods are notoriously favored by fraudsters as they are high value items that are easy to resell. Shoppers looking to score good deals on electronic goods have the tendency to search via third party sites to find the best bargain, enabling fraudsters to easily market their stolen goods for discounted prices and enjoy a nice pay off.

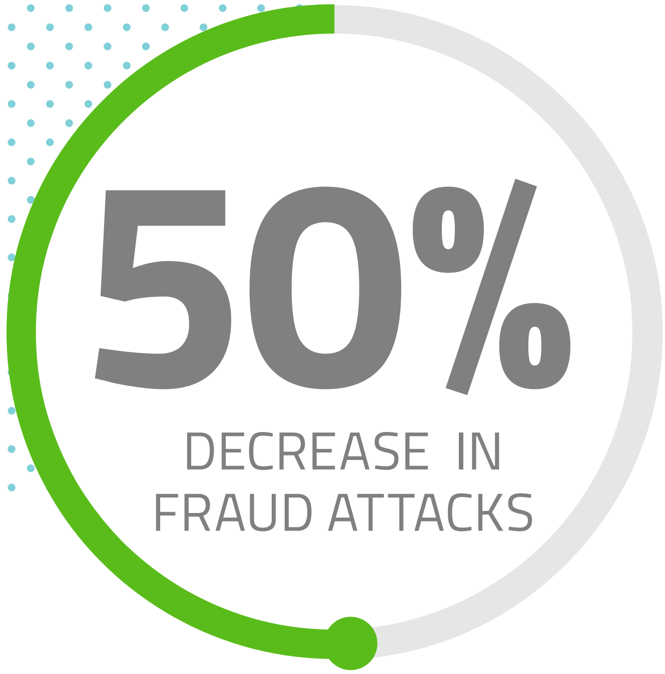


41%

INCREASE IN FRAUD ATTACKS

Food & Beverage

This is the third year in a row that fraud attacks against the online food and beverage industry has seen an increase. This year, attacks against these businesses **increased by 41%,** with the main culprit for this rise connected to abuse related to policies. This policy abuse refers both to professional fraudsters abusing food and beverage platforms, as well as to instances of “friendly fraud” — or what customers would simply refer to as “savvy shopping” — in which consumers open multiple accounts to leverage discounts or coupon codes. As the industry continues to be a targeted sector, the challenge moving forward will be striking a balance between safeguarding against fraud and abuse, while also understanding how to maintain customer loyalty in a competitive market.



Home & Garden

A relatively new industry, as more brick and mortar businesses shift their wares online, the home and garden industry has shown a **decrease of 50% over the last year.** Home goods are not easy to monetize, since it is much more difficult to coordinate in-store pickup for large items and fly under the radar. As such, only the very ambitious fraudsters who are able to create reseller or “backdoor” selling businesses that capture these types of items remain players in this industry.

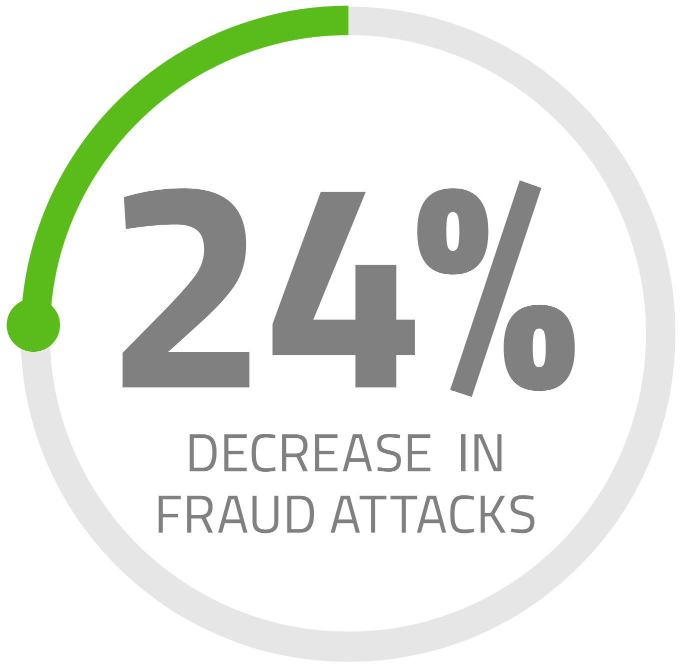
5%
INCREASE IN
FRAUD ATTACKS

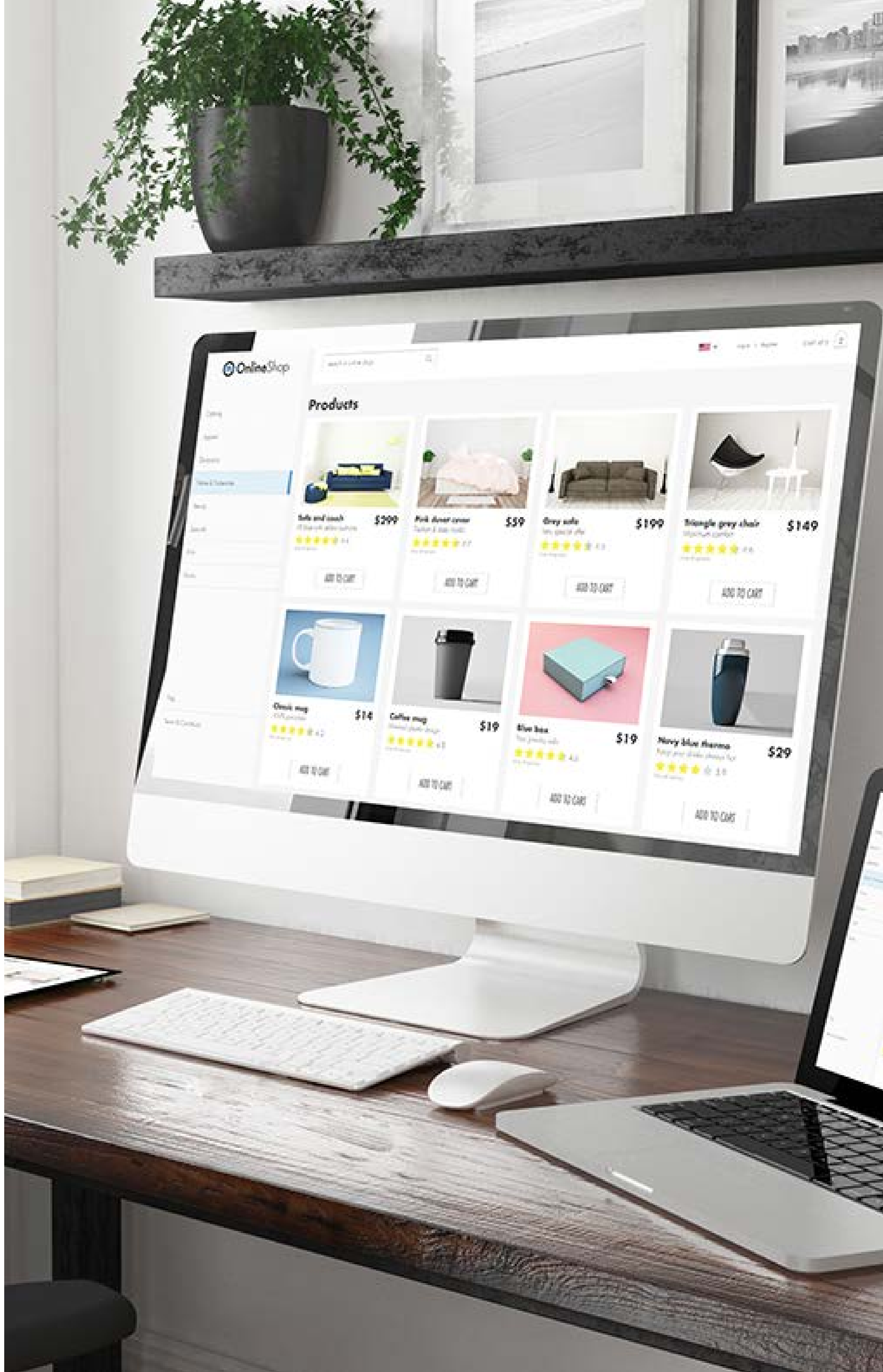
Jewelry

Fraud attack rates against the jewelry industry (balanced by the merchant model), showed an **increase this year by 5%.** Online fraudsters tend to favor this industry since just one successful attack (given the high value per item) can yield an extremely lucrative payout. Merchants in this industry should look to protect their platforms, since attacks against this industry persist despite current fraud prevention methods.

Marketplaces

As online marketplaces grow, and more major retailers consider launches into online marketplaces, this is an important industry to watch. Fraud attack rates against online marketplaces demonstrated a **24% decrease this year**, with more sophisticated fraudsters shifting to merchant-focused fraud attacks instead. That being said, a pervasive issue in this industry is *buyer-seller collusion*. Online marketplaces no longer lose money solely at the point of transaction as fraudsters are growing more sophisticated in how they exploit these platforms. The unique challenge here is that marketplaces require a holistic fraud prevention solution that can automatically and accurately determine good entities from bad. The reputation and integrity of the market platform itself are vital to protect, and they should be considered when selecting a fraud prevention partner. The type of buyer-seller collusion activity seen in this industry can be minimized through entity-based decisioning.





Travel

The travel industry encapsulates air travel, hotel and accommodations, and ground transportation and land travel. These subcategories present their own unique challenges and pain points. As such, we have separated them to best reflect the trends in each area.

61%
INCREASE IN FRAUD ATTACKS

Air

Fraud attack rates against airlines **increased over the last year by 61%**. This increase can likely be attributed to the rise in loyalty program issues and some related data breaches, such as the British Airways breach that impacted customer information from roughly 380,000 booking transactions made between August 21 and September 5 of 2018. With such immense wealths of data available, fraudsters are focusing their attentions on account-based attacks and other forms of abuse in addition to transactional fraud attacks.

10%
DECREASE IN FRAUD ATTACKS

Hotel

Attacks against hotels and accommodations have shown a **decrease by 10%** (balanced by the merchant model). Hotels have introduced friction-free experiences in order to provide their customers benefits and the best services. However, as a result of these more seamless experiences, there was a rise in fraud in this area, followed by countered efforts to increase friction in order to deter these fraudsters (thus the small decrease in rates).

38%
INCREASE IN FRAUD ATTACKS

Land

This year saw a rise in fraud attacks against **ground transportation by 38%**. This increase is attributed to the fact that car rentals and ride services apply less friction in their platforms (ease of pick up in parking, no ID required, etc.), in order to remain competitive in the market and for the perceived better customer experience. The push for an excellent and friction-free customer experience has created vulnerabilities in these platforms, which fraudsters have been targeting. As it relates to trains and buses, there has been a trend in local fraudsters abusing return policies. They simply cash in on their online tickets, i.e., at the train station, upon returns. This MO is incredibly lucrative, turning a stolen product into money with only meager effort, as compared to reselling, needed on the part of the fraudster.

Variety

Variety refers to more of the old style stores that capture a wide array of products and goods. A one-stop-shop for all consumer needs. This variety store is the present day equivalent to one dollar stores wherein they sell everything — ranging from notebooks to pillows to snack foods. Attacks against these types of stores have **increased by 50%** over the last year. The appeal of these types of stores is similar to the appeal captured in the apparel and accessories industry — it is easy to buy items in bulk and then resell them without raising flags with the merchant. The push of one-dollar stores from traditional brick and mortar models into online offerings is a rising trend in the digital market.

50%

INCREASE IN
FRAUD ATTACKS

The Customer Experience

The Customer Experience Reigns Supreme

Amongst the primary benefits is providing shipping options to their consumers. In a very competitive space wherein Amazon and other large marketplaces and companies offer 1-Click payment and same-day delivery, customer expectations have reached new heights. Instant gratification and a completely seamless experience is now the customer expected norm. As such, online merchants know they will be expected to provide this type of service in order to stay competitive. A fully automated fraud prevention solution is the only means to mitigate the possibility of fraud within the confines of this more streamlined system.

2X
AS RISKY
Standard Shipping
Express Shipping

Express Shipping

Express shipping is **about twice as risky** as Standard shipping where it used to be four times as risky.

3X
AS RISKY
Standard Shipping
Premium Shipping

Premium Shipping

Premium shipping used to be nearly seven times as risky as selecting a Standard shipping option, but data indicates this more expensive shipping option is **now only about three times as risky.** The decline in the fraud rates here can be accounted for by the rising mainstream expectation that customers have now become accustomed to expect near instant gratification. The overall denominator is growing as all merchants are shifting in order to provide this type of service offering, but likewise, so are the demands and expectations of customers.

Standard Shipping

When looking for specific products or items, customers today have a plethora of options. Therefore, the benefits that merchants provide need to be incredibly worthwhile to ensure brand loyalty and continued competitiveness in the market.

Sophistication in Shipping Fraud

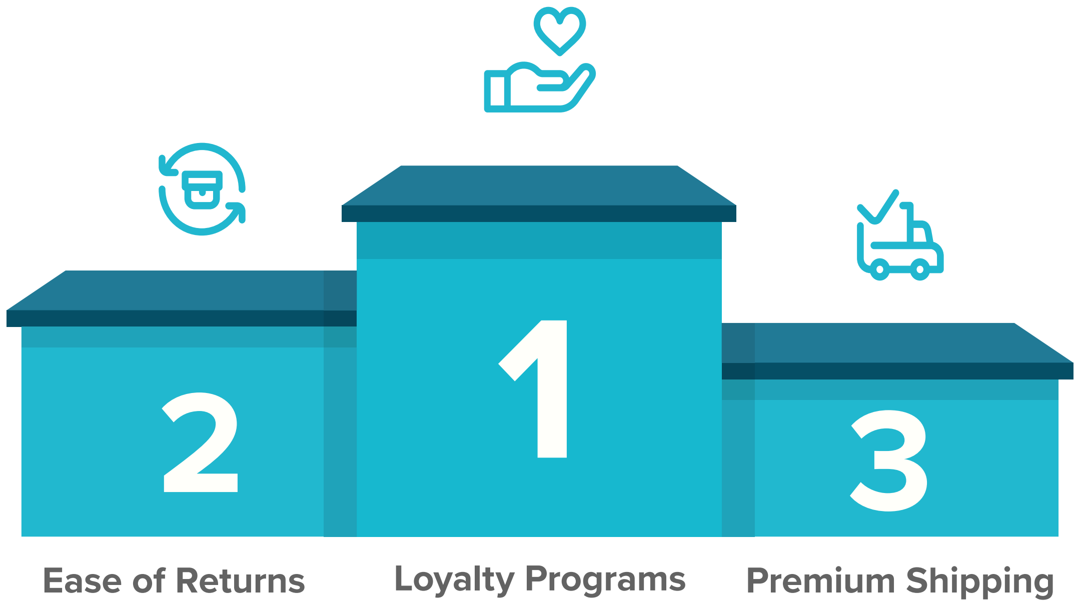
As more fraudsters find loopholes within improved customer experience to exploit for their own gains, re-routing fraud has become a growing phenomenon. As merchants begin to realize the vulnerabilities some of their streamlined offerings may provide, they have started to place limitations on the ability of shipping companies to change the shipping address on a package. Post-payment is a convenience that many merchants had previously offered in case their customers needed to change the delivery address at the last moment. This results in the gaining popularity of “hold at location” fraud, where fraudsters request the shipment to be held at the shipping company’s facility and then leverage fake IDs, mules (see BOPIS), or manipulate the sales clerks in order to receive the package to the new location.

Another tactic fraudsters have been favoring to exploit merchant shipping convenience is address manipulation. In these cases, fraudsters purposely mislead automated checks, like the Address Verification System (AVS), by changing only a part of the address to mismatch reality or to be insignificant enough to go unnoticed, creating a conflict between them. Through minor changes and circumvention of these types of processes, fraudsters are able to re-route items from their intended locations to drop spots that best suit them.

SPOTLIGHT

What Merchants Care About

As merchants expand their customer-centric offerings, they focus on how best to capitalize on specific benefits that underscore their ability to cater to customer needs and expectations. When polled, Forter merchants responded that Customer Experience offerings are key to their brands and businesses. Our merchants prioritized these types of offerings as follows:



Methods of Attack

Account Takeover (ATO)

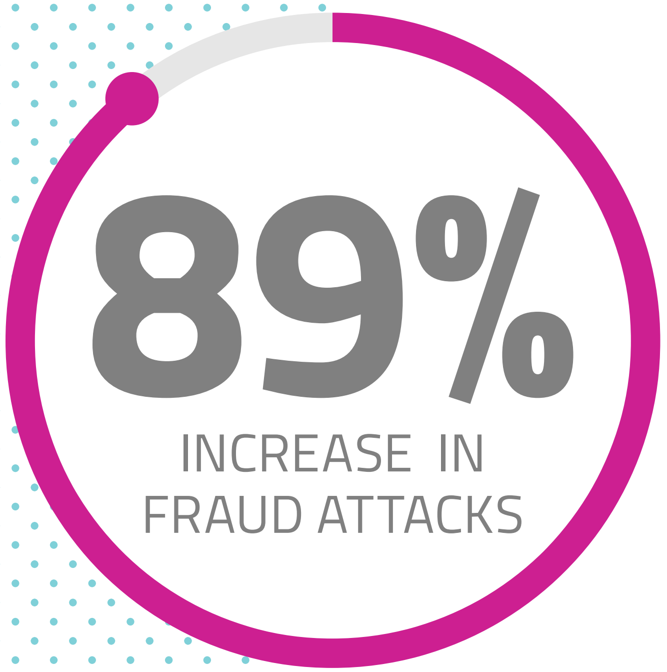
Account Takeover (ATO) attacks this year have shown a **decrease by 14%**. Fraudsters are shifting away from high volumes of indiscriminate attacks. Instead, their attacks are *growing in sophistication*. This accounts for the slight decrease in volume of ATO attacks. There has been a significant increase in the targeting, sophistication, and innovation of fraudsters. Fraudsters are getting more sophisticated in their attacks, and using more complex and difficult to detect monetization schemes. One and a half million victims of existing account fraud had an intermediary account opened in their name first. **This is 200 percent greater than the previous high.** When fraudsters do attack, their work is more fruitful and results in a higher payoff.

> Fraudsters are getting more sophisticated in their attacks, and using more complex and difficult to detect monetization schemes. One and a half million victims of existing account fraud had an intermediary account opened in their name first. This is 200 percent greater than the previous high.

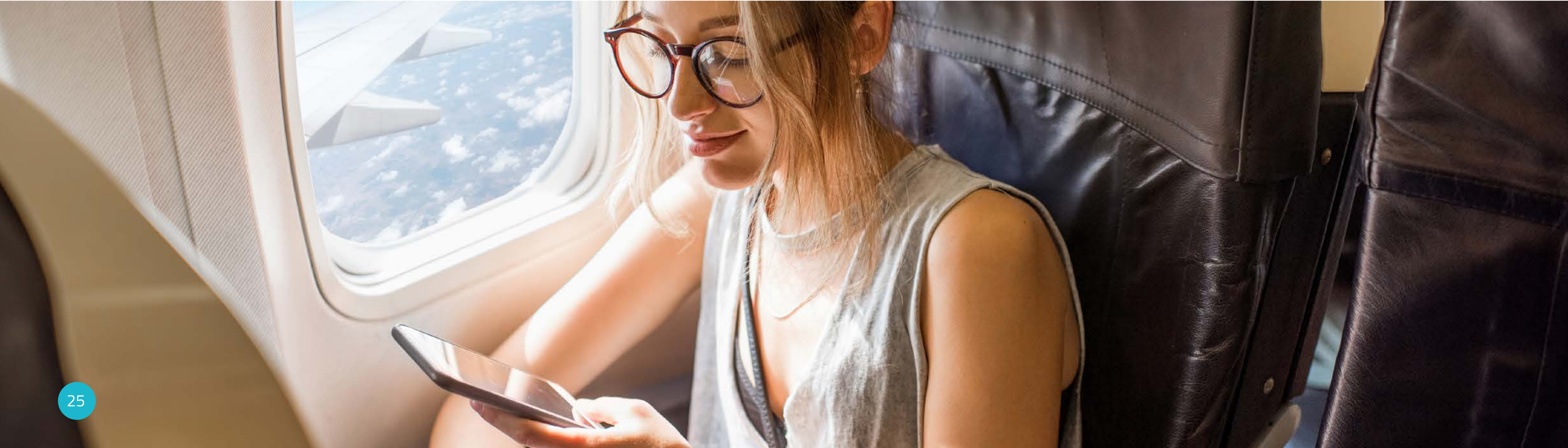
14%

DECREASE IN
FRAUD ATTACKS

Loyalty



Loyalty fraud is on the rise. Between Q2 2018 - Q2 2019, this method of attack **increased by 89%.** There has been a significant shift in how merchants position their offerings in order to capitalize on customer experience. The expectations of good, brand-loyal customers is to be recognized by their frequented shopping platforms and to sail through the shopping journey — no friction, no added obstacles. As a result of these widening customer expectations, merchants have a lower threshold for preventive measures that could create increased friction for their good shoppers. As a result, loyalty point programs become more vulnerable to opportunistic fraudsters. Points accrued in a customer's account are treated like digital goods — redemption is wholly conducted online, and requires no stolen credit card information to execute. Fraudsters are thereby able to leverage these points as "free" funding sources and given the minimal mitigation efforts by merchants, are able to consistently do damage without raising suspicions.



BORIS & BOPIS

(The Omnichannel Experience)

Buy Online Return In Store (BORIS)

The abuse of a merchant's return policies is a borderline fraud MO, since it is very hard to define or capture the true intent of a buyer. In other words, some returns are legitimately conducted by good shoppers and therefore adds value to the overall brand offering to good customers. However, by utilizing the ratio between the frequencies of returns and the different identities used, it can be established that among merchants who offer in-store returns, **6.2% of the return are highly likely to abuse the merchant's return policy.** While online returns have slightly decreased within the past year, Buy Online Return In Store **(BORIS) fraud has increased by 23%.** BORIS is easier to execute as there are minimal barriers to returning items in-store. Similarly, when customers present themselves in-store to bring back items, merchants likely err on the side of caution and accept the returns — aiming not to create friction or a poor customer experience.

That being said, the price tag of this kind of returns abuse is quite high. **Returns abuse has cost retailers in the United States more than $17B every year.** These costs range from losses incurred by item wear and tear, to operational costs for processing, shipping, restocking of items, as well as allocation of store personnel to returns and is weighed against the prospect of increasing sales. As merchants turn toward a more customer-centric goal, the importance of BORIS offerings to reward good customers will continue to grow. While this offering will be vital for merchants to stay competitive, it is also likely to create growing risks and heightened potential for financial losses.

23%
INCREASE IN FRAUD ATTACKS

BORIS & BOPIS

(The Omnichannel Experience)

Buy Online Pick Up In Store (BOPIS)

BOPIS is similarly a growing offering leveraged by merchants. To ensure merchants stay competitive in an expanding market, offering customers the ability to order items online coupled with the ease of in-person fulfillment greatly benefits their target audience. However, data indicates that in-person pickup fraud rates resemble the fraud rates online. **BOPIS fraud rates increased by 23%** rising YoY from Q2 2018 to Q2 2019.

In cases of BOPIS fraud a common MO leveraged by fraudsters is to use their victim's correct billing and personal details, ask for in-store pickup and then appear in-store while assuming the identity of said victim. In order to successfully pick up the stolen goods, the fraudsters then either present a fake ID of their victim, use mules who are close in age/appearance/or build to the victim, or sweet-talk store clerks into supplying the items.

BUY ONLINE PICK UP IN STORE (BOPIS)

23%

INCREASE IN FRAUD ATTACKS

Instrument Manipulation

Instrument manipulation, or the takeover of the entirety of the instrument itself, **has grown this year by 15**%. This incremental increase as a method of attack reflects how fraudsters shift as they compensate and leverage other MOs. However, with mobile devices and hardware continuing to be easy to access and increasingly affordable to procure, fraudsters will continue to turn toward this method of attack. By leveraging burner phones, virtual machines, bots, and remote desktop protocol (RDP), fraudsters are able to mask their activities, cloaking themselves from detection by less sophisticated fraud prevention systems.

15%
INCREASE IN
FRAUD ATTACKS

SPOTLIGHT

The Ultimate Instrument Manipulation

Over the course of this year, Forter witnessed a significant increase in Remote Desktop Connection (RDC) and RDPs being leveraged. Use of this type of technology personifies the very highest level of instrument manipulation, and in some ways it is most akin to the concept of the "invasion of the body snatchers." In the same way that the film "body snatchers" embodied the mannerisms, features, and looks of the bodies in which they snatched, RDPs operate similarly. It is a takeover of the entirety of the instrument itself — from behaviors, to specific technical features. RDP is a sophisticated way for fraudsters to cover their tracks and snatch another individual's instrument (body) to appear completely innocuous to fraud detection systems.

HOW IT WORKS

Remote Access Attacks (Computer Takeovers)

Fraudsters typically maliciously gain control over computer via:

1. *Remote Access Trojans* (RAT) which prompts the PC user to install malware that gives the fraudster remote access to the individual's computer.
2. Exploitation of vulnerabilities in existing RAT programs (such as team viewer) to gain access to device.
3. Methods of social engineering (i.e. a technical support scam).

Once fraudsters have gained access to a victim's computer, they will use it as a base from which to conduct fraud. In simple fraud, the affected device will just be used as the platform for the fraud, gaining a legitimate IP and device in a relevant location for the victim's address. In more sophisticated fraud, the attacker will use a keylogger (surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard), or check for accounts and passwords saved on the computer in order to gain access to the computer owner's card details. In these types of cases the fraud victim is also the computer owner and for all basic cyber indications will appear the same (i.e. same IP and device).

30%

INCREASE IN FRAUD ATTACKS

Identity Manipulation

Identity manipulation as a method of attack **has grown by 30% this year.** In identity manipulation, fraudsters aim to gain stolen Personally Identifiable Information (PII) of legitimate individuals (often stolen from a third party) to conceal their true identities. Fraudsters often execute this method of attack through sophisticated acts of social engineering.

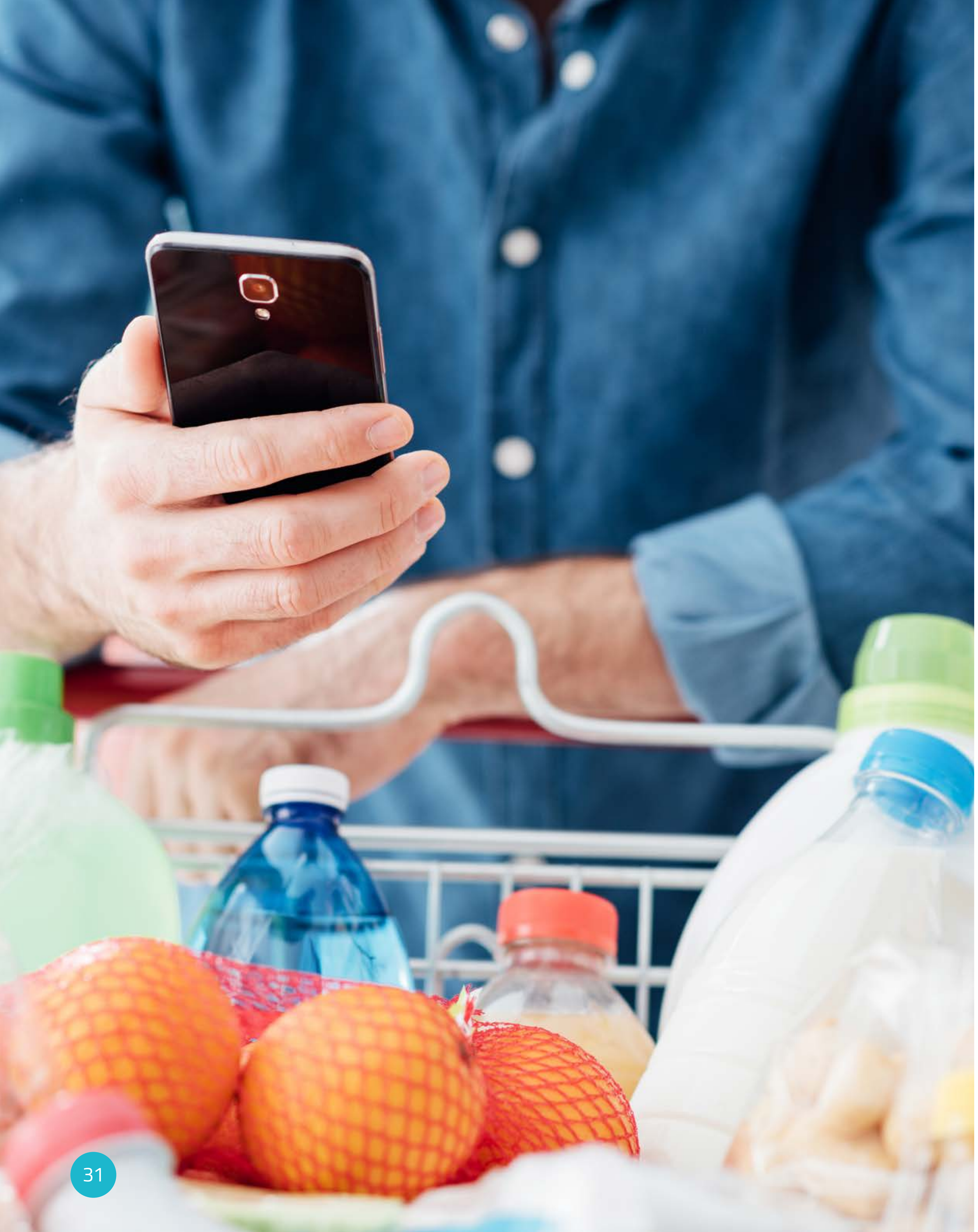
In committing acts of social engineering, fraudsters will use deception to manipulate legitimate individuals to divulge confidential or personal information to leverage for fraudulent purposes. For example, a fraudster will open a domain similar to a reliable domain used by the legitimate card holder through which to conduct fraud: john.doe@bankofamerica.com and john.doe@bankofamerica.us.

Repeat Offenders

9%

DECREASE IN FRAUD ATTACKS

This year again saw a decrease as a method of attack. **Decreasing by 9% from last year**, fraudsters are finding more sophisticated methods of attack to exploit rather than attempting to launch repeated attacks against the same platform. As highlighted in the growth of instrument manipulation, fraudsters are investing more in technological advances and tools through which to launch their attacks — the intention being to be more targeted in their efforts, yielding bigger and better payoffs. Instead of leveraging multiple attacks in which only some may be successful — think automated bot attacks — they are investing more in singular attempts that will evade prevention systems and prove more lucrative.



Coupon

Coupon abuse saw an **increase of 10% this year**. This small increase points to ongoing oversharing of coupon codes by users on business platforms and merchants who still do not focus enough on fraud prevention efforts in this area. In an effort to better serve their customers and increase traffic and shopping on their sites, merchants often extend discount codes to new and loyal shoppers. Retailers take losses on these discounted purchases, especially if shoppers abuse refer-a-friend scenarios and proliferate the coupon codes widely. Furthermore, their online ecosystem becomes clouded with one-time use email addresses.

10%
INCREASE IN
FRAUD ATTACKS

Collusion

This year saw collusion rates **increasing by 32%**. As best exemplified in marketplaces, this is a growing phenomenon wherein fraudsters work together in order to boost each other's sales within online marketplaces or other platforms. Collusion efforts can diminish the sanctity of online marketplace ecosystems and creates difficulty for businesses lacking identity-linking capabilities to determine the veracity of their users.

32%

INCREASE IN FRAUD ATTACKS

Fraud Around the World

As global digital commerce continues to rise — nearing $3 trillion in 2018 — understanding the particular pain points in specific global markets is increasingly vital to merchants and their internal teams.

Europe, the Middle East, Africa (EMEA) & Asia Pacific (APAC), and Latin America (LATAM)

Different regions are characterized by different customer behaviors and different fraud trends. As such, data we see throughout these regions is unique and based on some of the following attributes:

Seasonality

While EMEA's buyer population is virtually all located in the Northern Hemisphere and focused in Europe, APAC's and to some extent AMER's population is spread more widely. Ultimately, this impacts buying patterns specifically within travel (air, land, and accomodations).

Holidays

While the holiday season in both AMER and EMEA (consisting mainly of Europe and Russia), tends to be towards the end of the year (including "special" dates such as Cyber Monday and Black Friday), holidays in APAC are spread across the calendar a bit longer, focused mainly between September until February. These holidays include Christmas, New Year's, Local New Year, and the most celebrated shopping spree in the world - Single's Day.

Data Breaches

Historically data breaches included mainly the United States (i.e. Marriott and Saks), they have hit Europe as well (British Airways) and in the last year APAC too (Cathay Pacific and Aadhar).

Locality and Language

While English is by far the prefered language among fraudsters, other commonly spoken languages such as Spanish or French tend to be popular as well. It is highly unlikely for someone who is not Chinese to utilize a Chinese card through a local website.

Cross Border

Fraud across regional borders is a bit more limited. AMER buyers focus on AMER websites, while EMEA buyers focus on EMEA websites and to some extent AMER websites and APAC websites (mostly non Europeans). APAC buyers focus on AMER and APAC websites.

Regional Variance

While AMER is comprised mostly of North America, English speaking buyers, and a minority of Spanish or Portuguese speaking LATAM buyers, EMEA is made up of three continents and dozens of languages. Similarly, APAC is the most densely populated region consisting of many dozens of different languages.

Global digital commerce continues to rise — nearing $3 trillion in 2018

A deeper dive into some of the industries favored by fraudsters...

APPAREL & ACCESSORIES

Fraud attack rates against the apparel industry rose by 60% in the Americas. EMEA shows a much lower increase, by 13%, while rates in APAC show almost no increase at all (APACs numbers are much higher as is).

AMERICAS	60% ↑
EMEA	13% ↑
APAC	0%

DIGITAL GOODS

EMEA and APAC show an increase, with rates consistent at 13% and 21%, respectively. This is mainly driven by the increase in gift card popularity and offset by a decrease in the Americas of 23%.

AMERICAS	23% ↓
EMEA	13% ↑
APAC	21% ↑

ELECTRONIC GOODS

Different trends appear in different regions. The increase in the Americas by 19%, is offset by the slight decrease in EMEA (4%) and the steeper decrease in APAC (37%).

AMERICAS	19% ↑
EMEA	4% ↓
APAC	37% ↓

JEWELRY

The jewelry industry showed an increase in fraud attack rates in the Americas (25%), offset by a 14% decrease in EMEA.

AMERICAS	25% ↑
EMEA	14% ↓
APAC	0%

Growing Markets, Growing Your Business

In general, there are particular countries widely considered by most businesses and fraud professionals as “high risk.” While this may historically have been true, data indicates that while there are more fraud attempts that occur in countries like Indonesia, Nigeria, and Vietnam, the bulk of the transactions originating from these countries are still legitimate shoppers. Typically, merchants view transactions originating from these countries as “NO-GO” since these higher risk countries have a fraud rate of up to 5 times higher than rates in the United States. Even still, the vast majority of the transactions emanating from these countries are indeed legitimate. **While merchants have dismissed whole regions in the past, these areas actually represent the potential of growing and burgeoning markets, where businesses have yet to expand to out of fear of fraud**. These countries are the ones that comprise the fastest growing digital retail markets and should be considered as legitimate business opportunities wherein merchants can truly grow.

Financial Inclusion in a Modern Age

We live in a global time, where technology minimizes the distances between people across different countries, regions, and cultures. This notion also applies when considering and discussing what people buy, where they buy it, and where they are from. Today, people in Indonesia can order as many packages of Haribo gummy bears they want — there is no need to look for a specific store, or location. As this trend continues to be true, the value of being a financially inclusive business is becoming far more important. In order to remain competitive, businesses need to ensure their fraud prevention solution is built to enable clients worldwide to access and receive their items, to be approved if they are truly legitimate, and more than anything else — to have a seamless shopping experience. It should be the goal of every merchant to be branded as a business that enables consumer experiences and shopping across the globe.

Methodology

With over $140 billion in e-commerce transactions, the Seventh Edition Forter Fraud Attack Index encapsulates the most extensive research ever conducted in this field.

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

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

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

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 the merchants.

2

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

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

Where F_i is the number of fraud transactions for merchant *i* and *Ni* is the number of transactions for merchant *i* and *M* is the number of the 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.

FORTER®

ABOUT FORTER

Forter is the leader in e-commerce fraud prevention, protecting over $140 billion in online commerce transactions for over 500 million consumers globally from credit card fraud, account takeover, identity theft, and more. The company's identity-based fraud prevention solution detects fraudulent activity in real-time, throughout all online consumer experiences.

Forter's integrated fraud prevention platform is fed by its rapidly growing Global Merchant Network, underpinned by predictive fraud research and modeling, and the ability for customers to tailor the platform for their specific needs. As a result, Forter is trusted by Fortune 500 companies to deliver exceptional accuracy, a smoother user experience, and elevated sales at a much lower cost.

Forter is backed by $100M of capital from top-tier VCs including Sequoia, NEA, and Salesforce.

https://www.forter.com