





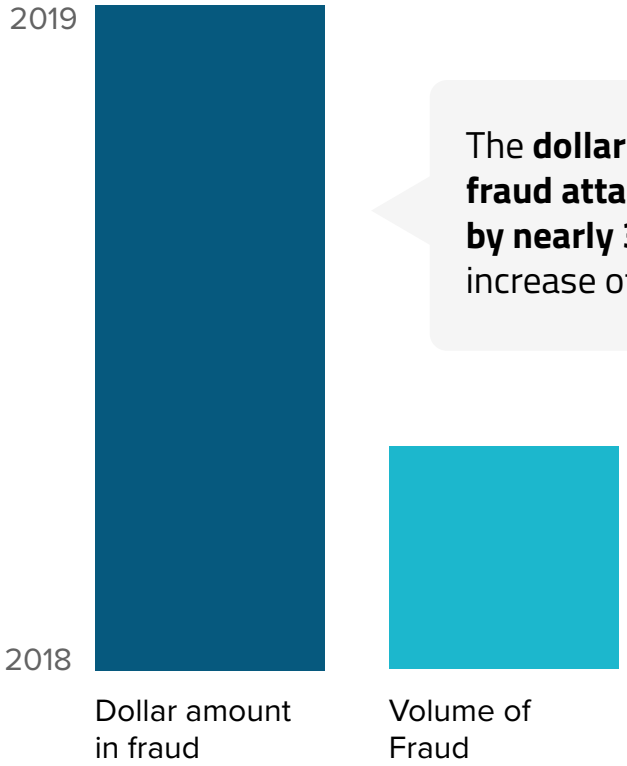

FORTER®

Fraud **Attack** Index

EIGHTH EDITION ▪ APRIL 2020

Year to Year

H2 2018 vs H2 2019



The **dollar amount in fraud attacks increased by nearly 3x** the rate of increase of volume of

This period also saw overall **fraud attacks increase by 19%.**

Highlights

Executive Summary

Customers shop and engage with their favorite brands in a variety of ways. In-store, online via their desktop, tablet, mobile devices, or all of the above at different times. Consumer expectations of their favorite brands are on the rise. Current events are likely to intensify the acceleration towards digital transformation as retailers address the impact of a global pandemic. Retailers must be prepared to contend with this new norm of customer experience where instant gratification, immediate fulfillment, and heightened personalization are expected, no matter how or where customers shop.

As commerce evolves, so too do fraudsters' methods of attack and exploitation. A rising level of sophistication in attacks and fraud and abuse methods comes at a time when user experience is key to overall business success. There can be a tension between a merchant's need to manage risk and their customers' expectation of seamless interactions throughout their path to purchase and fulfillment. To ensure brand survival in an increasingly competitive market, retailers must be able to deliver friction-free customer experiences while also protecting their business.

To achieve this it is imperative to understand the evolution of online fraud and abuse trends. New forms of fraud and abuse, no longer merely at the point of transaction, require businesses not only tore-examine their approach to opportunistic online criminals, but also to assess their threshold for abusive behaviors committed by legitimate customers. Methods of fraud and abuse are becoming more focused, more targeted, and poised to do greater damage than ever before. Retailers must understand how to better prepare their businesses and protect their customer ecosystem while delivering an exemplary consumer experience.

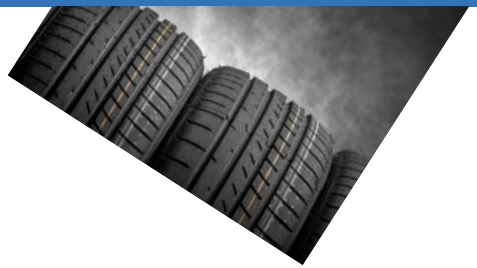


Table of Contents

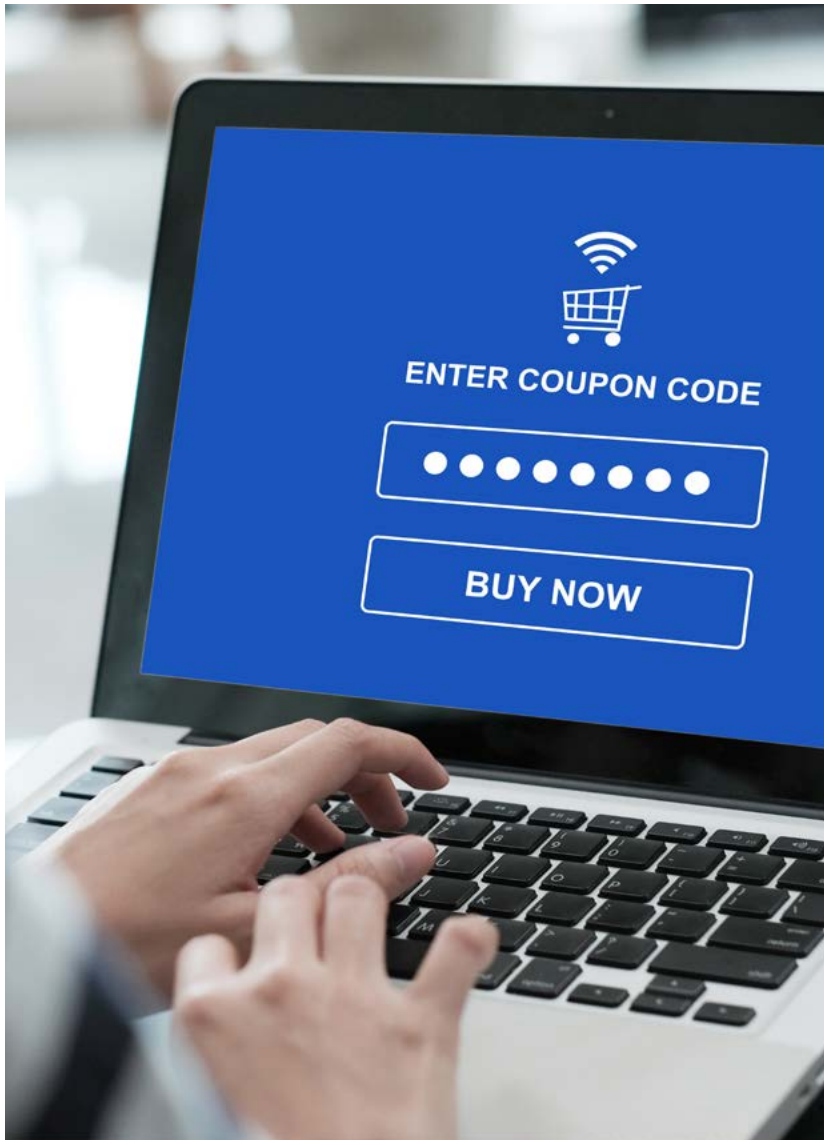
Year to Year	2
Highlights	3
Executive Summary	4
About this Report	6
Industry Breakdown	7
Striking the Right Balance	25
Methods of Attack	32
The Way Forward	39
Methodology	41

About this Report

The Eighth Edition of Forter's Fraud Attack Index highlights changes within and across the dynamic world of online commerce. This report is based on the depth and breadth of Forter's robust database to examine shifting behaviors and trends in online fraud attacks across global industries.

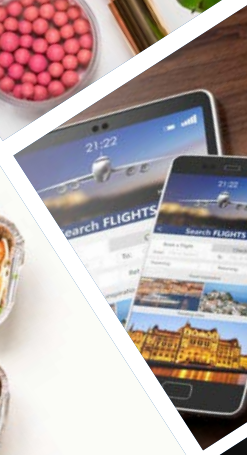
This report reveals fraud attack rates, rather than successful fraud. The data reported exposes current fraud and abuse patterns across a variety of global industries. This report aims to arm retailers with a deeper understanding of the current commerce climate, payment trends and rising vectors of account fraud and abuse, and to better equip them with the ability to ensure their businesses and customers are better protected from the most common fraud and abuse methods and vulnerabilities in the coming months and year.

With over $150 billion in e-commerce transactions, the Eighth Edition Forter Fraud Attack Index encapsulates the most extensive research ever conducted in this field.



Industry Breakdown





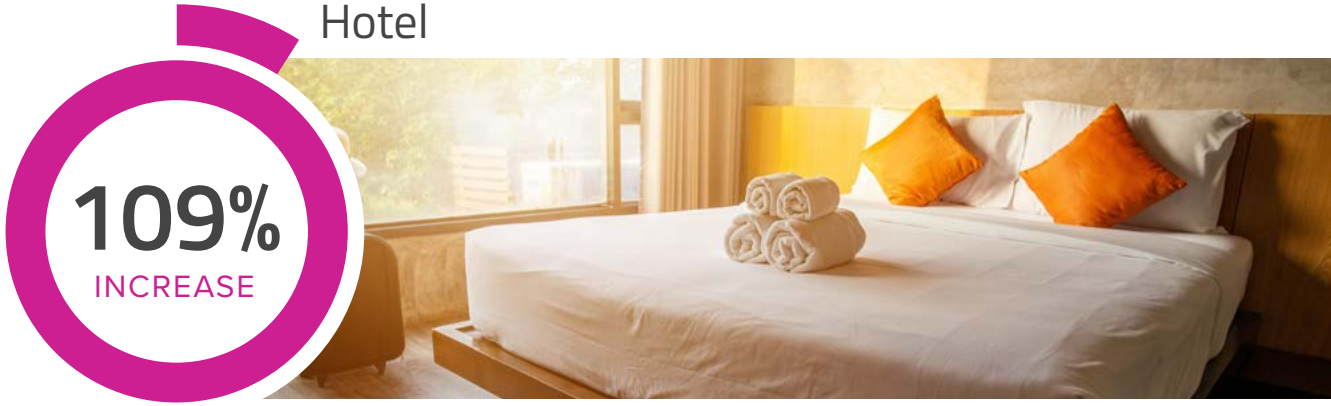


Travel

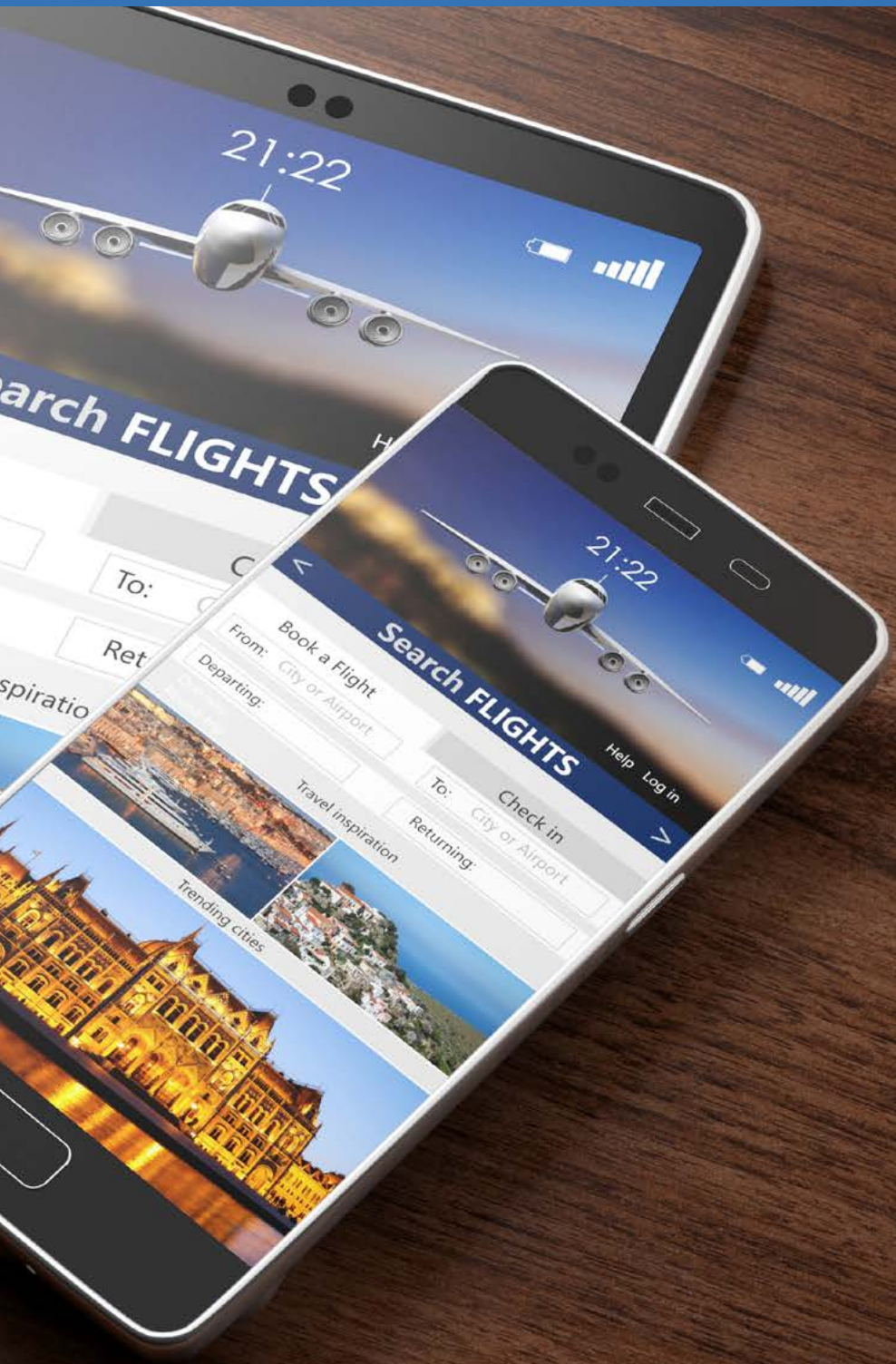
The travel industry encapsulates air travel, online travel agencies (OTAs), hotel and accommodations, and ground transportation, land travel, and parking. These subcategories present their own unique challenges and pain points. As such, we have separated them to best reflect the trends in each area.

Air

Hotel



Ground Transportation



TRAVEL

72%
INCREASE

Air

Fraud attack rates against airlines **increased between H2 2018 - H2 2019 by 72%**. Data breaches and increased focus on **loyalty program fraud** are major contributing factors to this increase over the last year. Airlines have also suffered from a rising level of sophistication of fraud attacks. Fraudsters are leveraging reputation takeover (RTO, see **Forter's Seventh Edition Fraud Attack Index for more details**) and account takeover (ATO) attacks more frequently. Likewise fraudsters adapt their behaviors to better blend into good traffic. Instead of booking last-minute trips (which can often be a sign of potential suspicious activity), fraudsters are now booking their travel further in advance of the actual date of actual departure, making it more difficult for airlines and OTAs to distinguish fraud from legitimate customer activity.

TRAVEL

Hotel

Attacks against hotels and accommodations have shown an **increase of 109% between H2 2018 - H2 2019**. The prevalence of increasingly “friction-free” experiences for check-in to hotels have contributed to this increase. Fraudsters are taking advantage of these improved customer benefit offerings to slip into the legitimate bookings. This improved and seamless experience accounts for the rise in fraud in this area. Counter efforts that followed to increase friction in order to deter these fraudsters resulted in such a diminished customer experience, that major hotel chains had to remove them, therefore re-exposing their businesses to increased risks. Online criminals also increasingly capitalize on travel package purchases where they can better blend in as legitimate buyers and are also able to target bigger payouts in just one attack.

TRAVEL

Ground Transportation

H2 2018 - H2 2019 saw a **rise in fraud attacks against ground transportation by 86%**. 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 friction-free customer experiences has created vulnerabilities in these platforms, which fraudsters have been targeting. Recent months have highlighted a notable increase of "card testing" activities within ride sharing platforms. Fraudsters use stolen credit cards in small amounts ($4 / $5 per transaction) to determine if the card is valid. Policy abuse in the form of coupon and heavy referral abuse has been on the rise within parking services. Abusers aim to park for free by spamming contact lists to enjoy the referral bonuses or discount codes associated with the service.

Money Services & Cryptocurrency

Money services and crypto remain a growing industry and an attractive target for fraudsters. There has been a **90% increase in fraud attacks between H2 2018 - H2 2019**, as the ease of cashing out makes this an even more desirable industry for fraudsters to target. Fraudsters can skip a complicated process to monetization as they're able to simply cash out immediately on financial transactions.

Variety

Variety refers to the old style stores that capture the “one-stop shop” concept for all consumer needs. Attacks against these types of stores have **increased by 42%** between H2 2018 - H2 2019. 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.

Food & Beverage

The online food and beverage industry, including grocery, Quick Service Restaurants (QSRs), and meal delivery, again saw an increase in fraud attacks.

Between H2 2018 - H2 2019, attacks against these businesses increased by 32%, with the main culprit for this rise connected to policy abuse

These are 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 thereby abusing business policies. Referral codes and loyalty program discounts for valued customers enhance food and beverage brands’ reputation and differentiates them from other companies. However, merchants are discovering that these benefits are not only extremely popular with their best and most loyal customers, but also with fraudsters and good customers who are abusing the system. (See “Customer Experience: Loyalty”).

Beauty

The industry saw a **13% increase**, and as reported in this year's fraudster wishlist. The beauty industry has seen a consistent rise both in online activity and fraud attacks over recent years. This burgeoning online industry is drawing more attention from legitimate online shoppers and online fraudsters.

Lipstick specifically was a highly targeted product, seeing attacks 7 times the normal rate.

Fraudsters also favored higher value products including eye shadow palettes and perfumes.

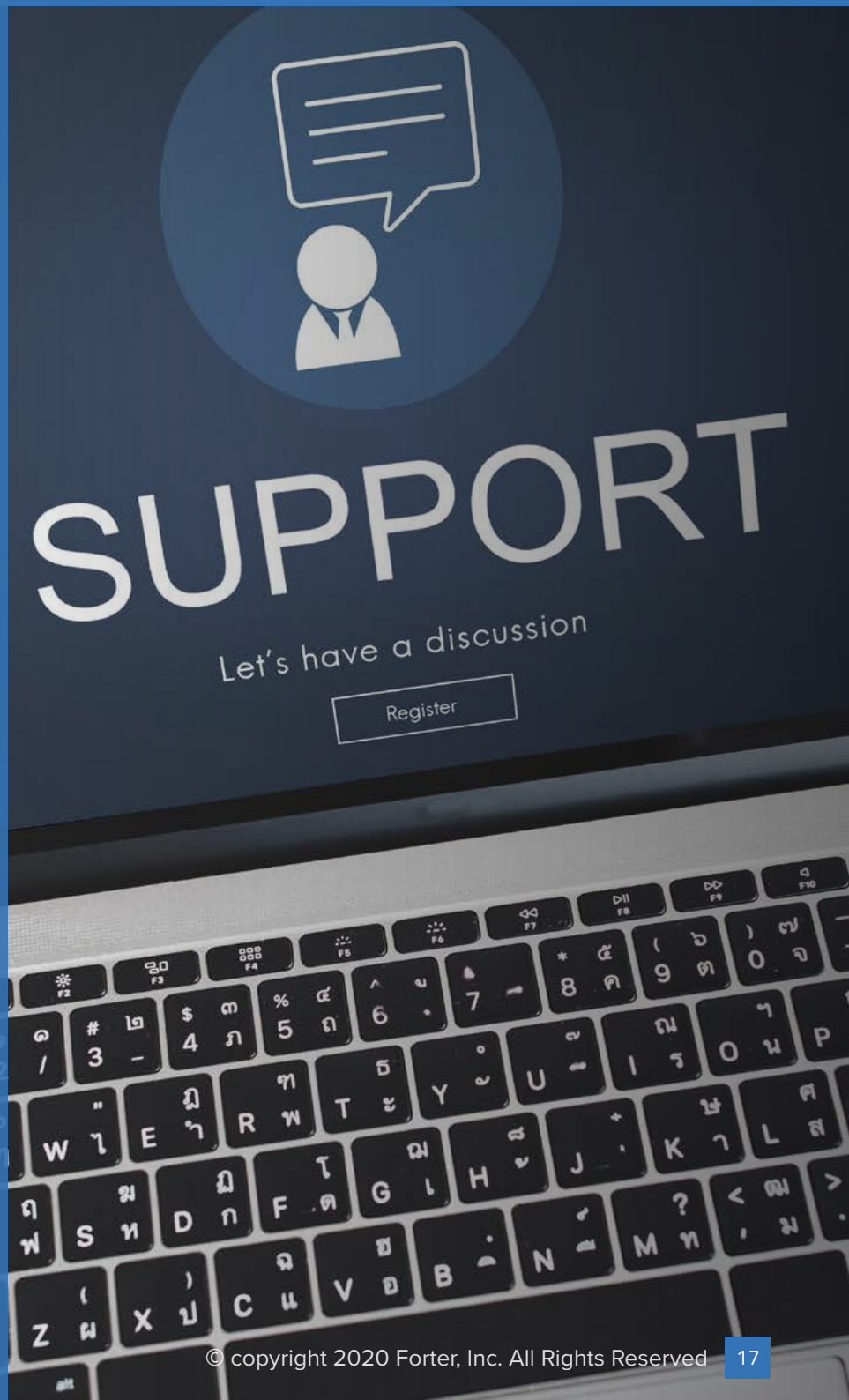
Apparel & Accessories

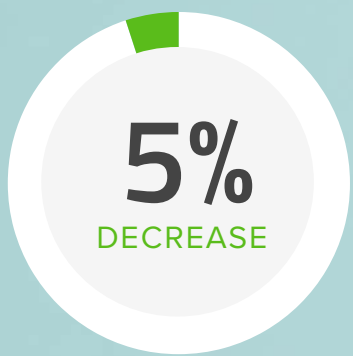
Fraud attacks on the online apparel and accessories industry **increased by 9% from H2 2018 - H2 2019**. Fashion merchandise never goes out of style. Consequently online fraudsters are easily able to resell these items. Typically, fraudsters buy this merchandise and turn a profit by reselling the items for near retail price to shoppers looking for the best bargains. Online criminals also tend to select items such as purses or accessories (sunglasses, eye wear, scarves, etc.) that do not require exact sizing to augment their ability to resell items. More sophisticated fraudsters who commit device takeover attacks target higher-end merchandise (see instrument manipulation in the Methods of Attack section).

SPOTLIGHT

Social Engineering

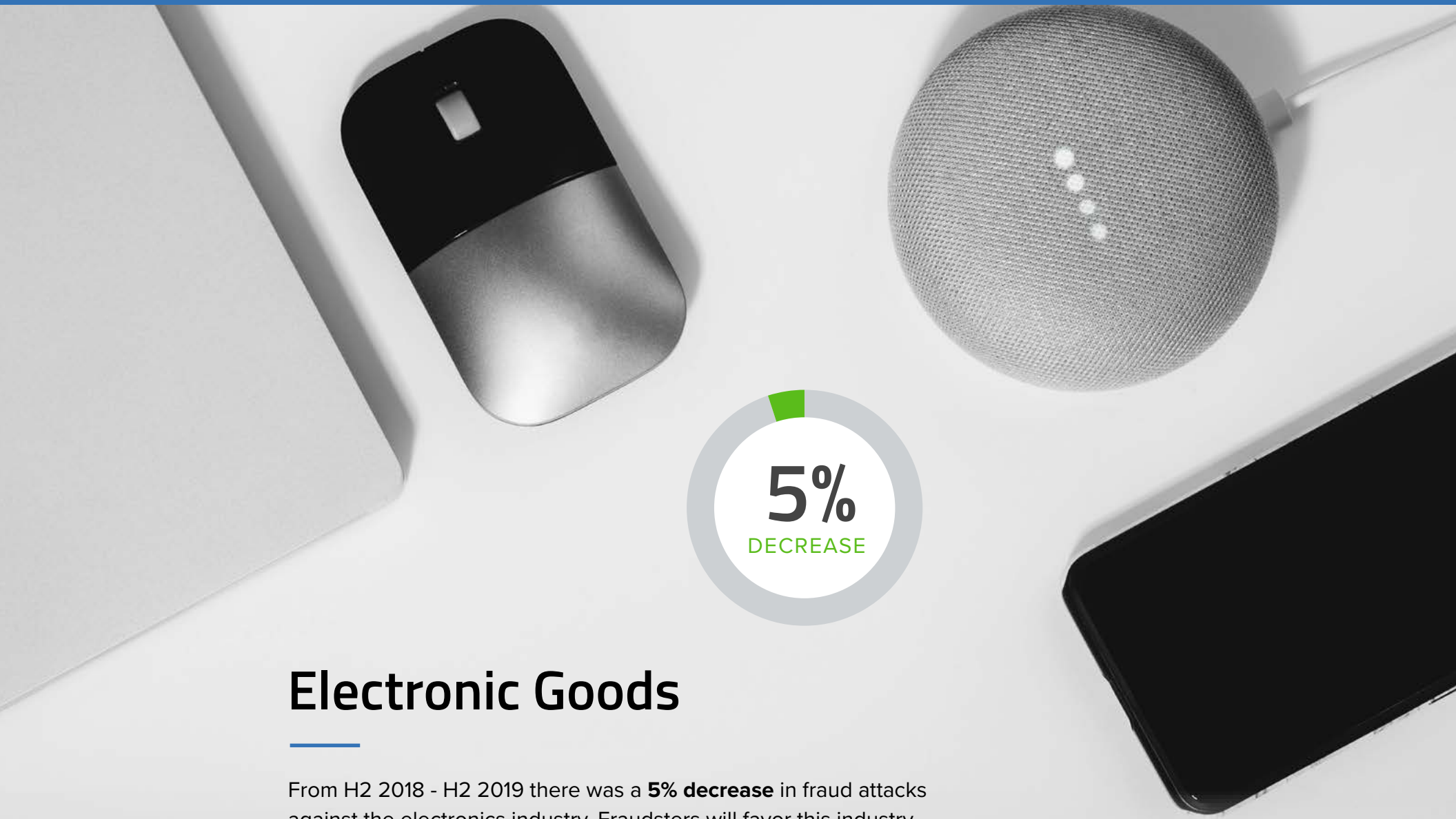
An emerging phenomenon among online criminals has been their attempts to contact and manipulate their victims to expedite their path to payout through social engineering. A sophisticated fraud scheme run by Indian fraudsters appeared in a global marketplace marked by a persistent phone scam targeting older individuals. Fraudsters directly contacted the victims, posing as Apple, Amazon, or eBay support team members (these teams are often located in India) to help troubleshoot the victims' online shopping experience. By sending a link for the victim to click through, the fraudster gains remote access and controls the victim's mobile device. They follow by asking for credit card and other personal details. The fact that these fraudsters target victims' mobile devices is a rather sophisticated way for fraudsters to cover their tracks. This mobile device take over is more rare and often more difficult to identify. These fraudsters were therefore able to appear completely innocuous to fraud detection systems. They often target gift card sites due to the ease by which they can monetize these products.





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. Digital goods include e-books, downloadable music, internet television and streaming media, fonts, logos, photos, gift cards, etc. This industry saw a slight **decrease by 5%** in fraud attacks. The smaller decrease coincides with a broader trend of *quality of attacks versus quantity of attacks.* Fraudsters are using more targeted and sophisticated attacks to elicit higher payouts, rather than focusing on increasing the volume of their attacks.

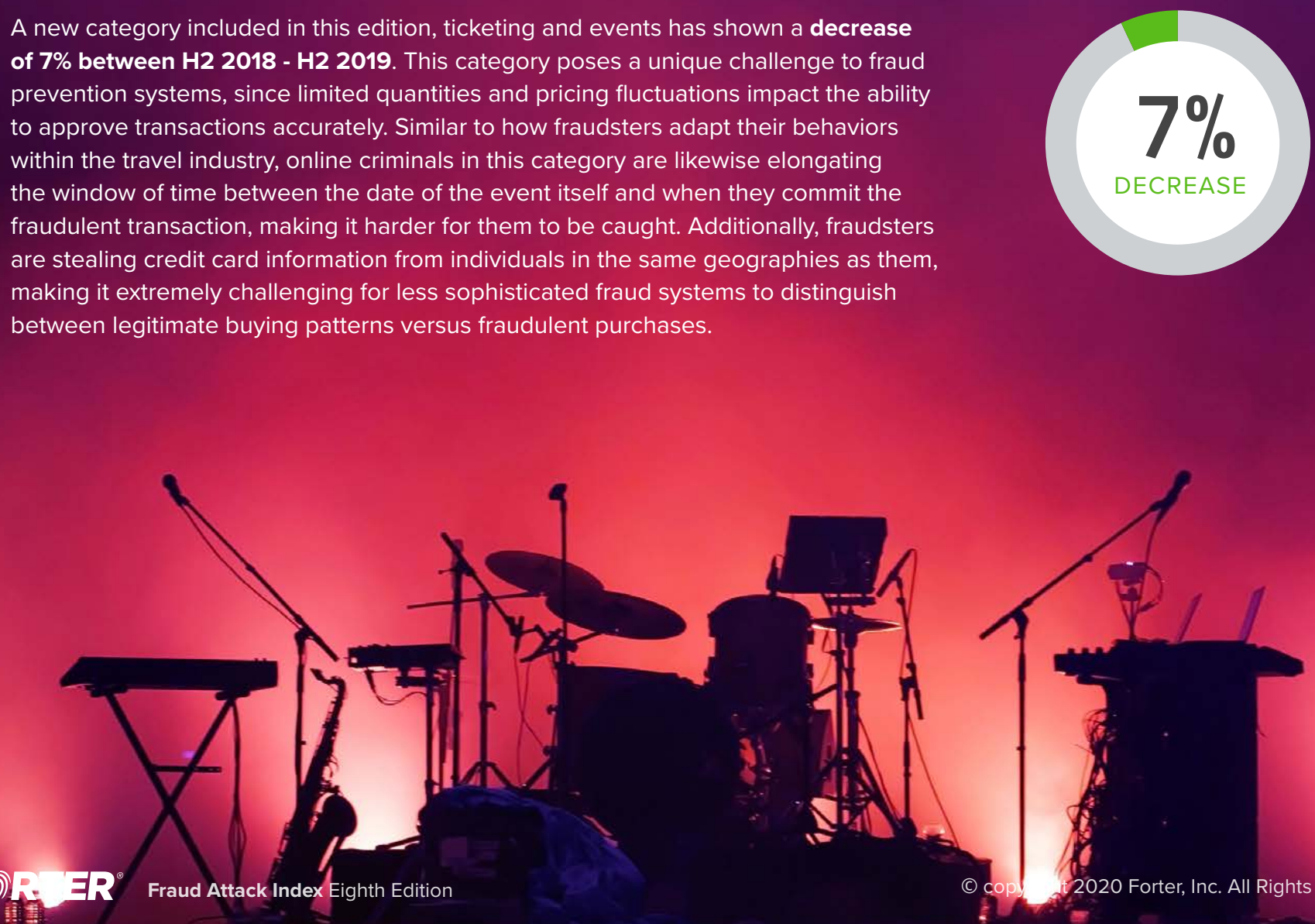


Electronic Goods

From H2 2018 - H2 2019 there was a **5% decrease** in fraud attacks against the electronics industry. Fraudsters will favor this industry since electronics tend to be high value items that are easy to resell. Shoppers looking to score good deals on electronic goods search via third party sites and marketplaces to find the best bargains, enabling fraudsters to easily market their stolen goods for below-retail prices and enjoy a nice pay off.

Ticketing & Events

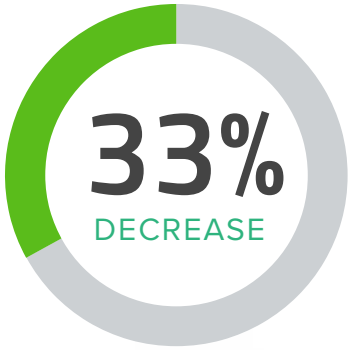
A new category included in this edition, ticketing and events has shown a **decrease of 7% between H2 2018 - H2 2019**. This category poses a unique challenge to fraud prevention systems, since limited quantities and pricing fluctuations impact the ability to approve transactions accurately. Similar to how fraudsters adapt their behaviors within the travel industry, online criminals in this category are likewise elongating the window of time between the date of the event itself and when they commit the fraudulent transaction, making it harder for them to be caught. Additionally, fraudsters are stealing credit card information from individuals in the same geographies as them, making it extremely challenging for less sophisticated fraud systems to distinguish between legitimate buying patterns versus fraudulent purchases.



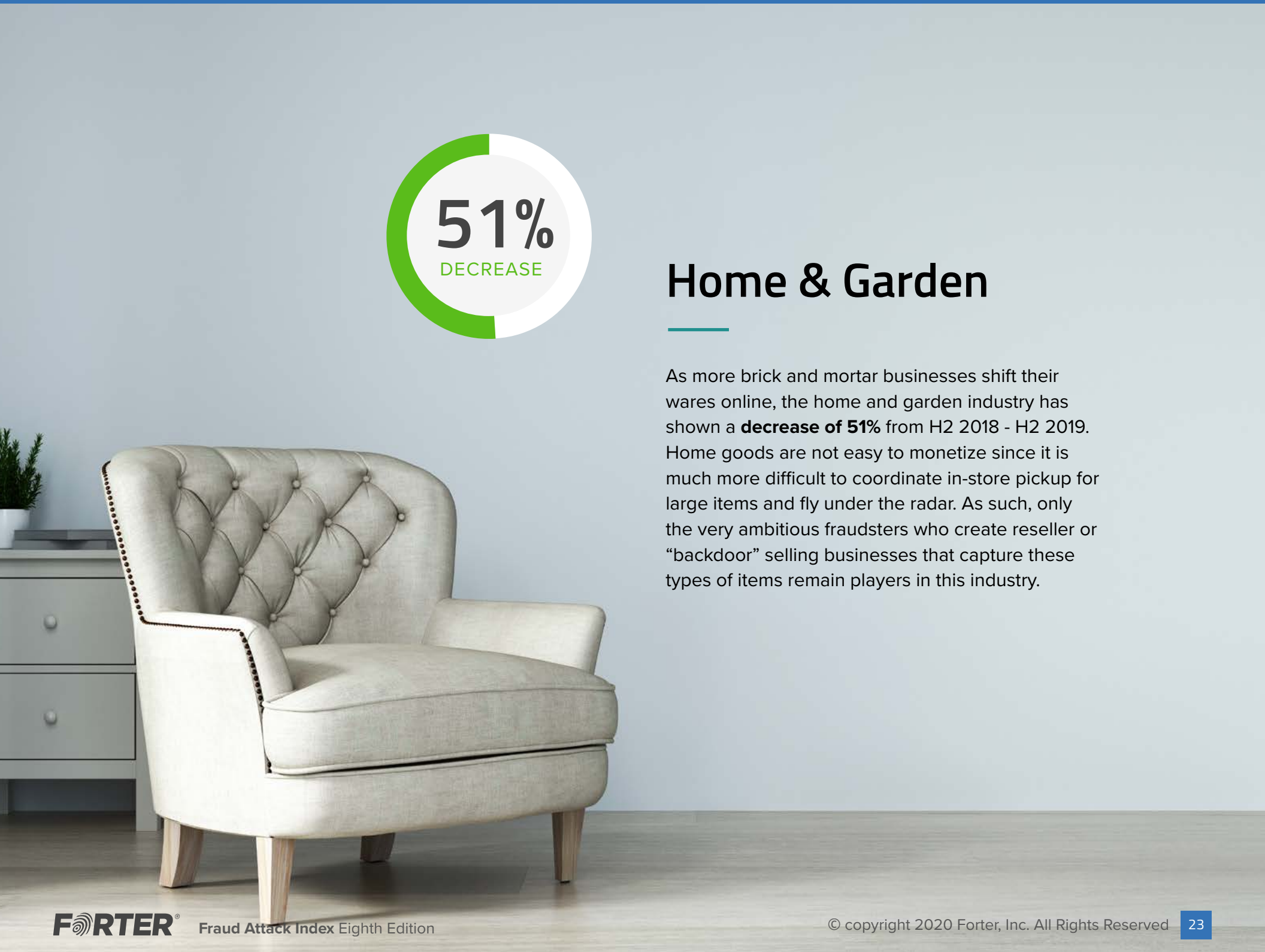
Jewelry

Fraud attack rates against the jewelry industry showed a **decrease of 25%** between H2 2018 - H2 2019. Online fraudsters in general tend to favor this industry since just one successful attack (given the high value per item) can yield an extremely lucrative payout.

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 **33% decrease** from H2 2018 - H2 2019, with more sophisticated fraudsters shifting to merchant-focused fraud attacks instead. Recently, fraudsters have been focusing more acutely on specific sellers where they find vulnerabilities and targeting more appealing products as well (e.g. hacked iPhones).

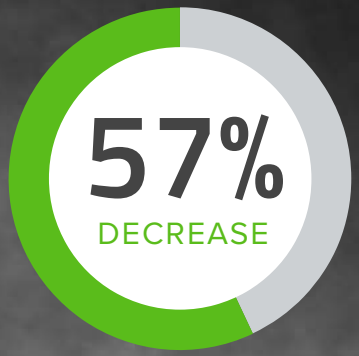


Home & Garden

As more brick and mortar businesses shift their wares online, the home and garden industry has shown a **decrease of 51%** from H2 2018 - H2 2019. 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 create reseller or “backdoor” selling businesses that capture these types of items remain players in this industry.

Auto Parts

Fraud attacks in this industry **decreased by 57%** from H2 2018 - H2 2019. Monetizing merchandise is more difficult in this category and therefore less popular amongst fraudsters. Typically, auto parts are more highly customized and therefore more difficult to resell given the specific requirements for parts to fit particular brands, makes, or models of vehicles.



Striking the Right Balance

A Best-in-Class Customer Experience, Protected from Fraud and Abuse

As customer expectations from their favorite brands reach new heights, merchants are expanding the ways in which they serve their best and most loyal customers. Primary benefits include offering more liberal returns policies, improving shipping or in-store pickup options, and building out more robust loyalty and reward programs. As merchants expand their customer-centric offerings for the most seamless experience and to keep their competitive edge, fraudsters and good customers are finding new vulnerabilities and vectors for abuse.

Returns Abuse

Nearly 1 out of 4 consumers (23%) have abandoned a shopping cart due to poor returns options and 3 out of 8 consumers (38%) indicate return policies have a major impact on their likelihood to purchase from any retailer. As such, merchants know that in order to keep customers shopping with their brand, they must be able to offer more flexible returns. However, as merchants expand their returns policies and aim to create more seamless experiences for their legitimate customers – returns abuse has been on the rise. Between H2 2018 - H2 2019 showed a **33% increase in returns abuse**. Striking the balance between offering returns benefits while accurately identifying abusive behaviors and actors, has proven a struggle for merchants. Without the proper precautions in place to protect their business, returns abuse can have a major impact on potential revenue.

CUSTOMER EXPERIENCE

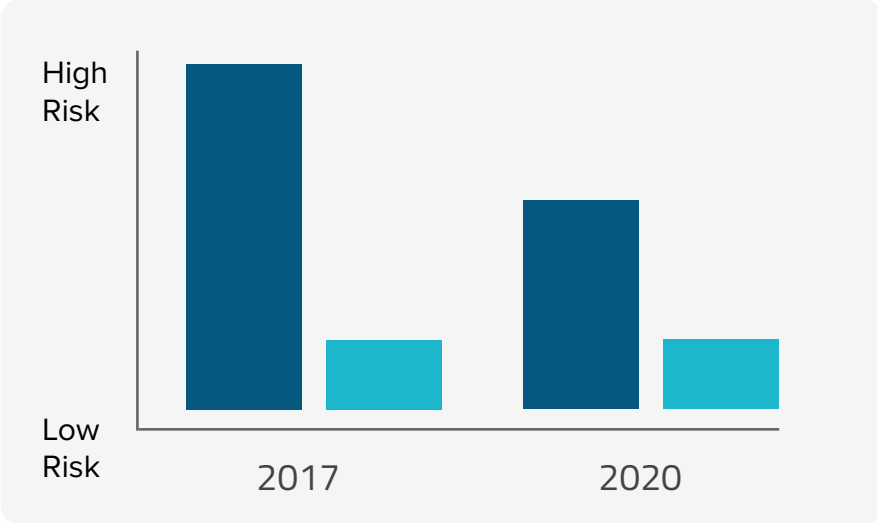
Item Not Received (INR) Abuse

Item Not Received (INR) abuse occurs when a customer receives their order but falsely claims that they did not receive it – usually to receive a full refund or another order at no additional cost. INR abuse can also occur when your business issues a refund to the customer following their claim, but the customer then also files a chargeback for an additional reimbursement on the same order – causing the business to lose twice. Forter has seen an **8% increase in INR abuse** between H2 2018 - H2 2019. Abuse of these kinds of policies or the threshold for tolerance of this type of activity varies from merchant to merchant. However without a nuanced, identity-driven abuse prevention solution in place, businesses lose on both the bottom and top lines.

Shipping Fraud

Premium Shipping

In 2017 premium shipping was 5 times as risky as a Standard shipping option. Our 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 become accustomed to near instant gratification.

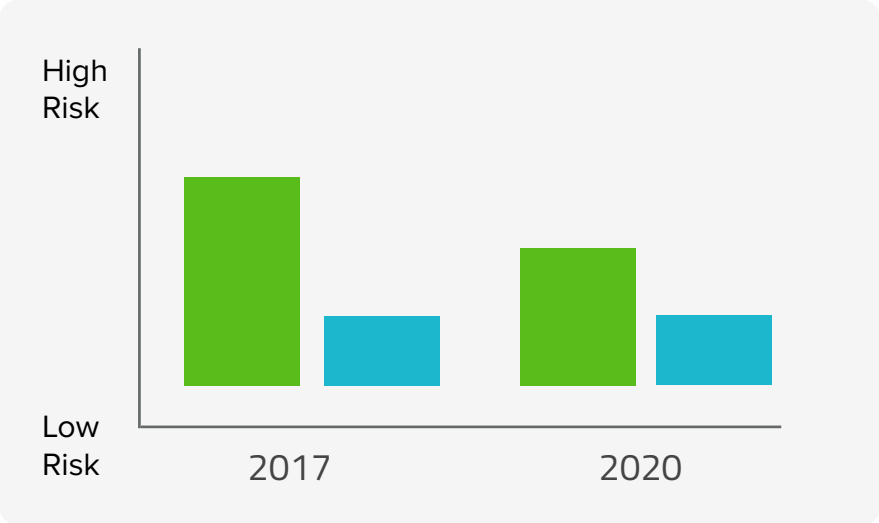


Express Shipping

Express shipping was about three times as risky as Standard shipping during 2017, but now is approximately two times as risky.

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.



CUSTOMER EXPERIENCE

Buy Online Return In Store (BORIS)

Buy Online Return In Store (BORIS) fraud and abuse has increased by 33%. BORIS is often easy 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 costs US retailers an estimated $24B annually. 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. This offering will continue to be vital for merchants to stay competitive, but businesses must ensure they have proper precautions in place to protect themselves from heightened financial losses.

CUSTOMER EXPERIENCE

Buy Online Pickup In Store (BOPIS)

Buy Online Pickup In Store (BOPIS) is similarly a growing offering leveraged by merchants to ensure their customers enjoy the most streamlined shopping experience. **BOPIS fraud rates increased by 62%** rising from H2 2018 to H2 2019.

In cases of BOPIS fraud a common MO leveraged by fraudsters is to use the 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.

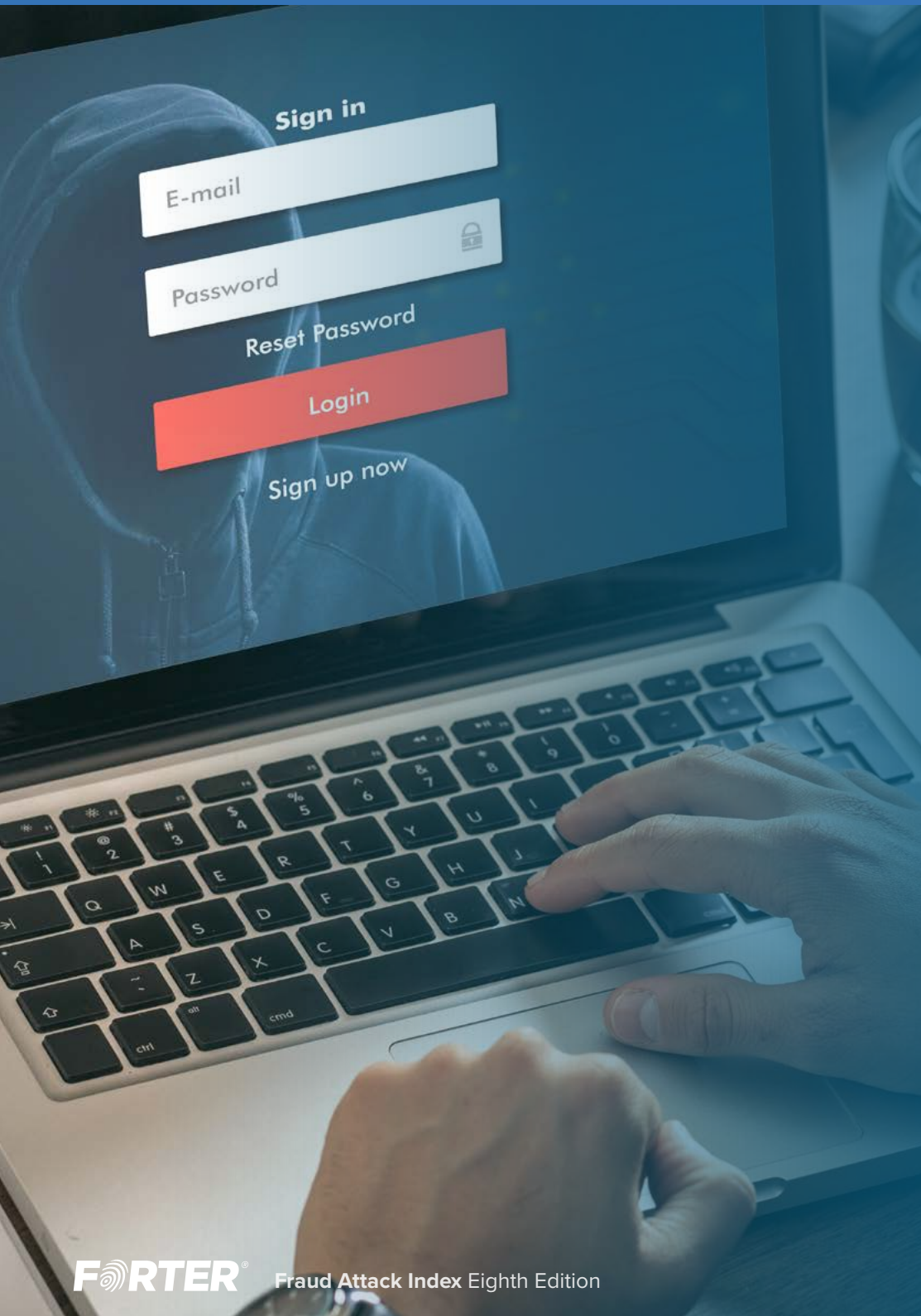
CUSTOMER EXPERIENCE

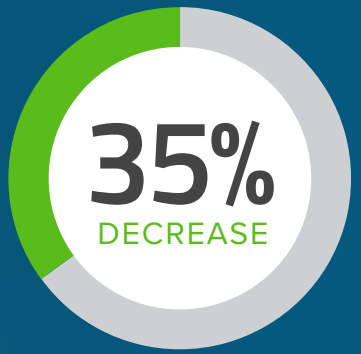
Loyalty Fraud

An increasingly competitive market means price promotions potentially encourage consumers to switch to the best offer. With 22% of consumers shopping exclusively with brands of whose loyalty programs they are members, retailers are taking note of the power behind building robust rewards programs[1]. However, fraud prevention in this area has lagged behind leaving loyalty point programs more vulnerable to opportunistic fraudsters. A shifting focus from pure transactional credit card fraud to account-based fraud and abuse puts customer loyalty programs at high risk. Points accrued in a customer's account are rarely closely monitored by either the customer or the merchant, leaving exploitation of the account and digital currency extremely vulnerable to fraudulent activity.

Loyalty fraud is on the rise. Between H2 2018 - H2 2019, this method of attack increased by 115%

Methods of Attack

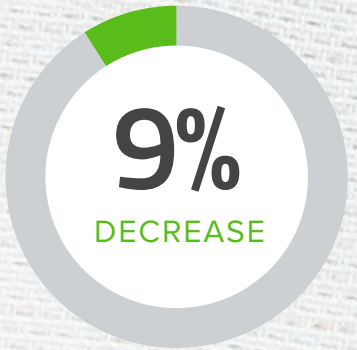


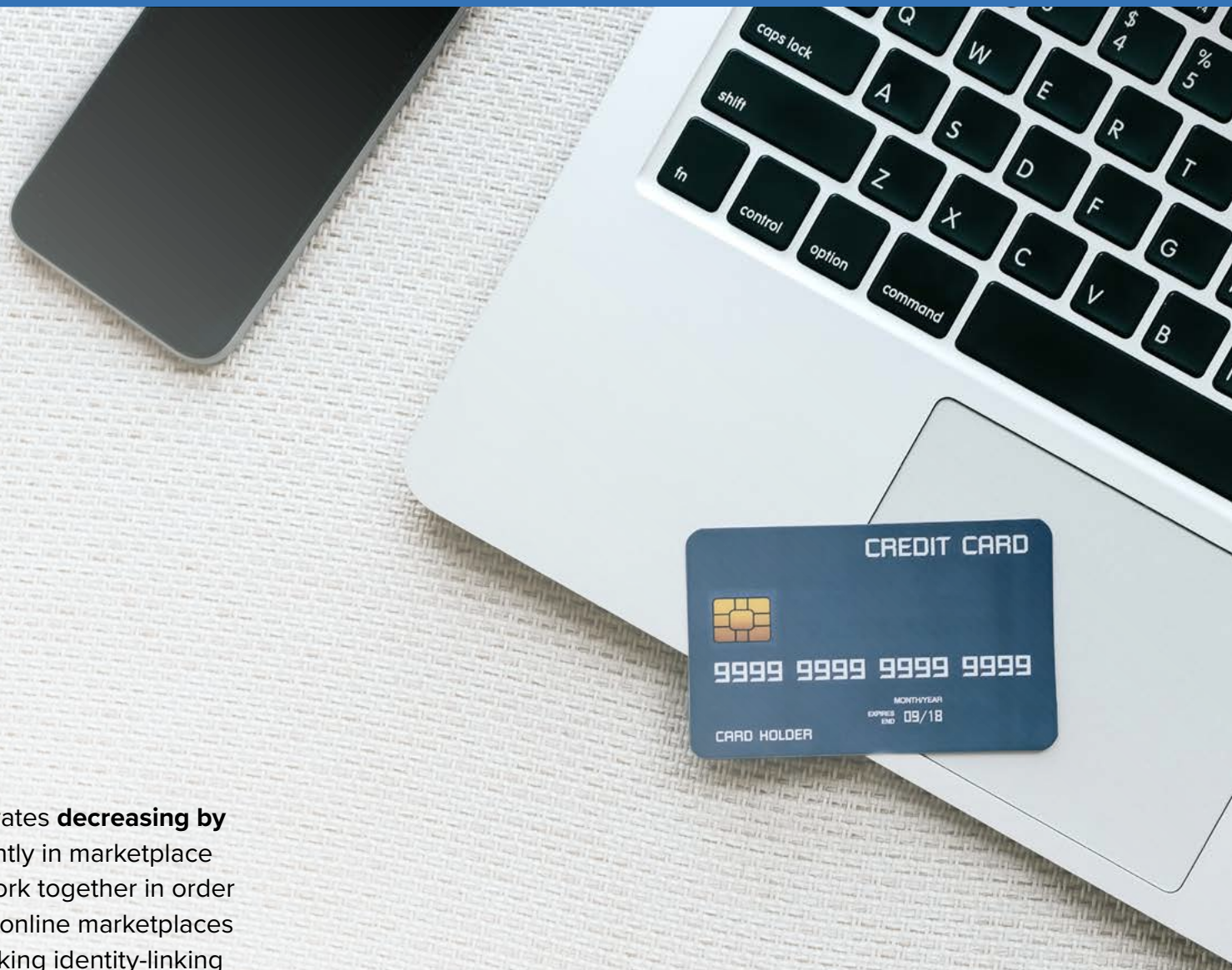


METHOD OF ATTACK

Account Takeover (ATO)

Account Takeover (ATO) attacks between H2 2018 - H2 2019 have shown a **decrease by 35%**. Fraudsters are shifting away from high volumes of indiscriminate attacks. Instead, their attacks are growing in sophistication accounting for the decrease in volume of ATO attacks. There has been a significant increase in the **targeting, sophistication, and innovation of fraudsters**. Fraudsters are getting more advanced in their attacks, and using more complex and difficult to detect monetization schemes.





METHOD OF ATTACK

Collusion

H2 2018 - H2 2019 saw collusion rates **decreasing by 9%**. Collusion occurs most frequently in marketplace environments where fraudsters work together in order to boost each other's sales within online marketplaces or other platforms. Businesses lacking identity-linking capabilities to determine the veracity of their users most acutely suffer from this type of activity.

METHOD OF ATTACK

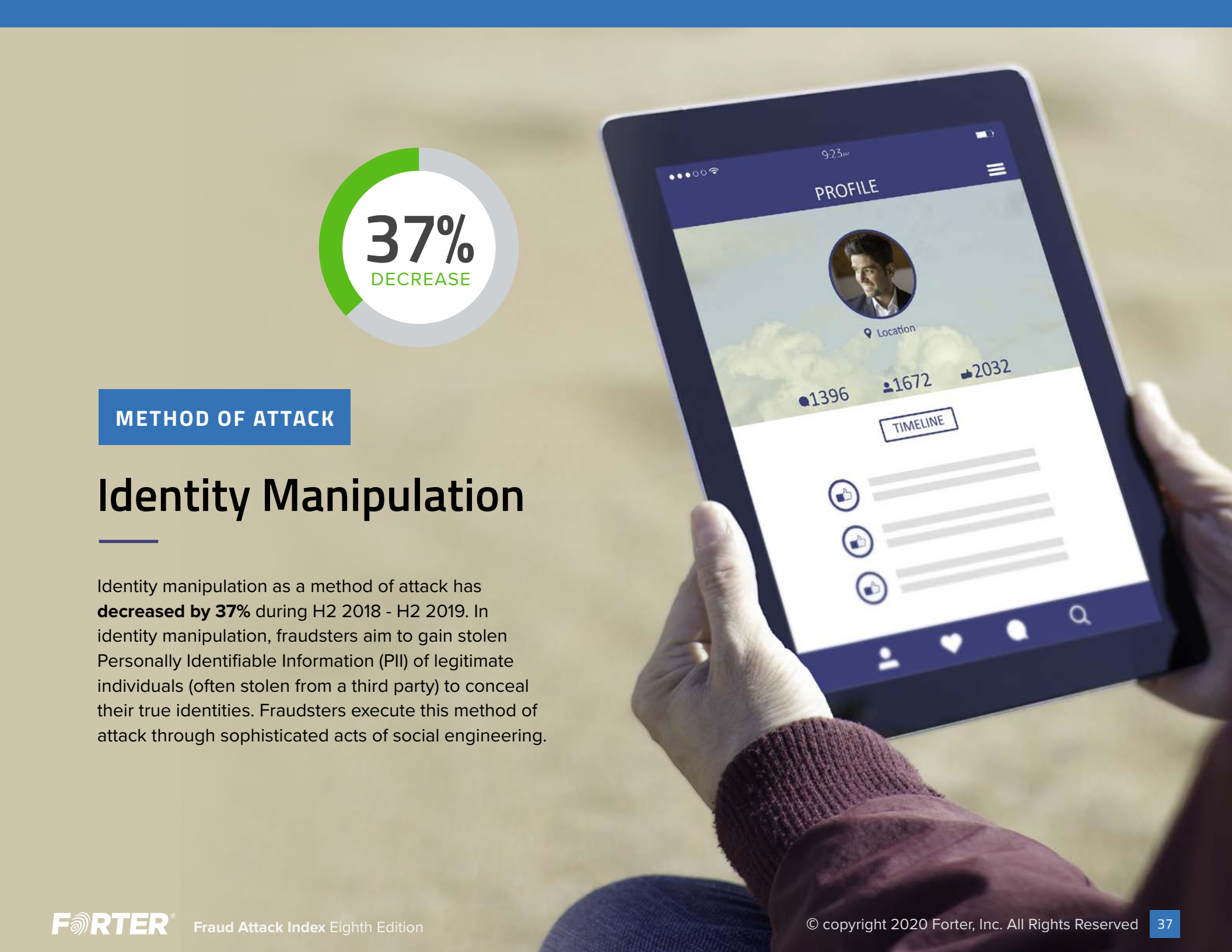
Coupon

Coupon abuse saw an **increase of 133%** between H2 2018 - H2 2019. This increase points to ongoing oversharing of coupon codes by users and merchants who are not able to put proper precautions in place to deter this kind of abusive behavior. Merchants aiming to better serve their customers often extend **discount codes to new and loyal shoppers**, however they risk absorbing losses on these discounted purchases, especially if shoppers abuse refer-a-friend scenarios and proliferate the coupon codes widely. Estimates put the cost of coupon abuse between $300 million and $600 million of losses per year[2].

METHOD OF ATTACK

Instrument Manipulation

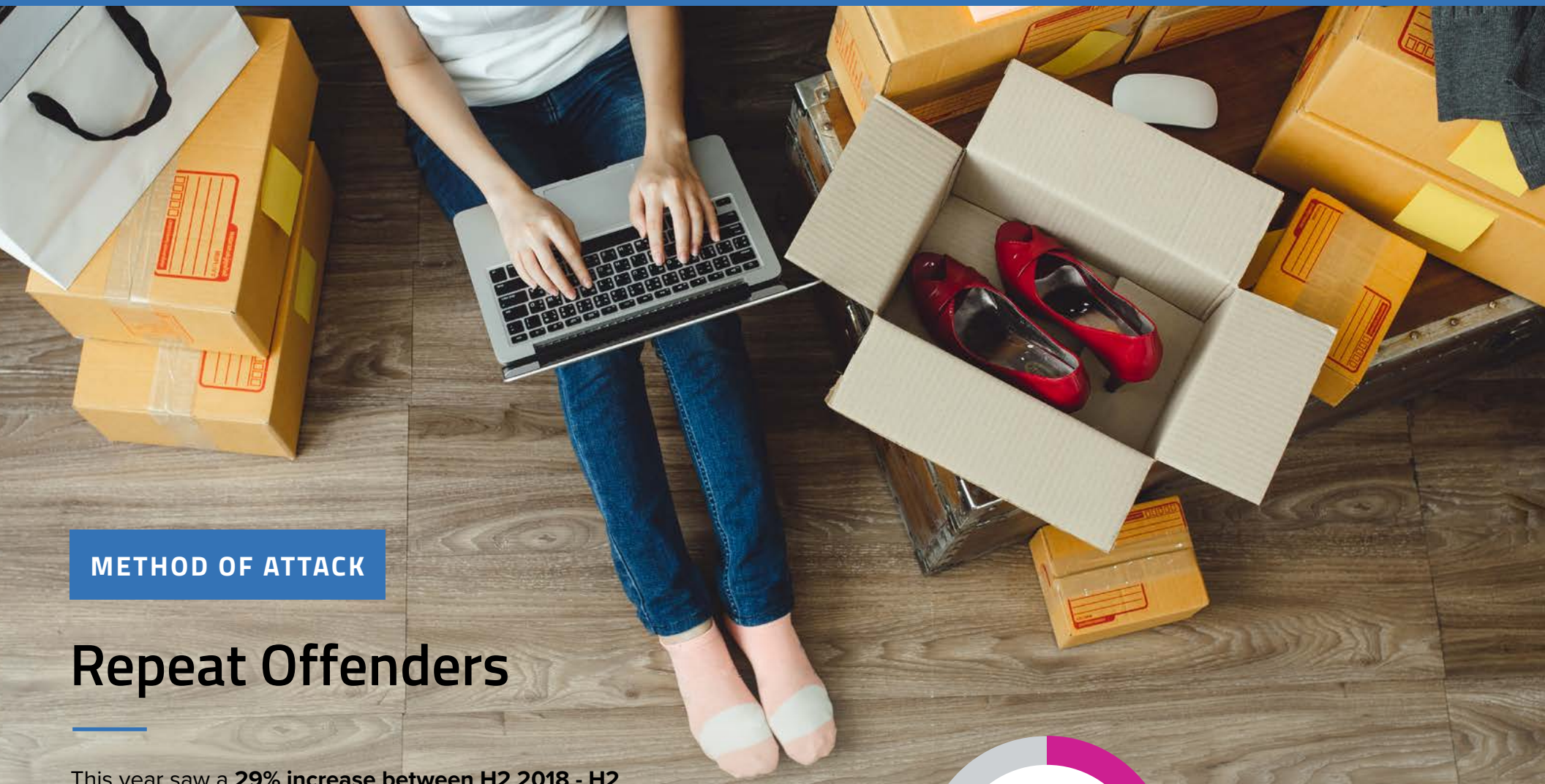
Instrument manipulation, or the takeover of the entirety of the instrument itself, has **grown between H2 2018 - H2 2019 by 57%**. This increase as a method of attack reflects growing sophistication and the ease by which fraudsters are able to access more affordable mobile devices and hardware. By leveraging burner phones, virtual machines, bots, and remote desktop protocol (RDP), fraudsters mask their activities, cloaking themselves from detection by less sophisticated fraud prevention systems.



METHOD OF ATTACK

Identity Manipulation

Identity manipulation as a method of attack has **decreased by 37%** during H2 2018 - H2 2019. 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 execute this method of attack through sophisticated acts of social engineering.



METHOD OF ATTACK

Repeat Offenders

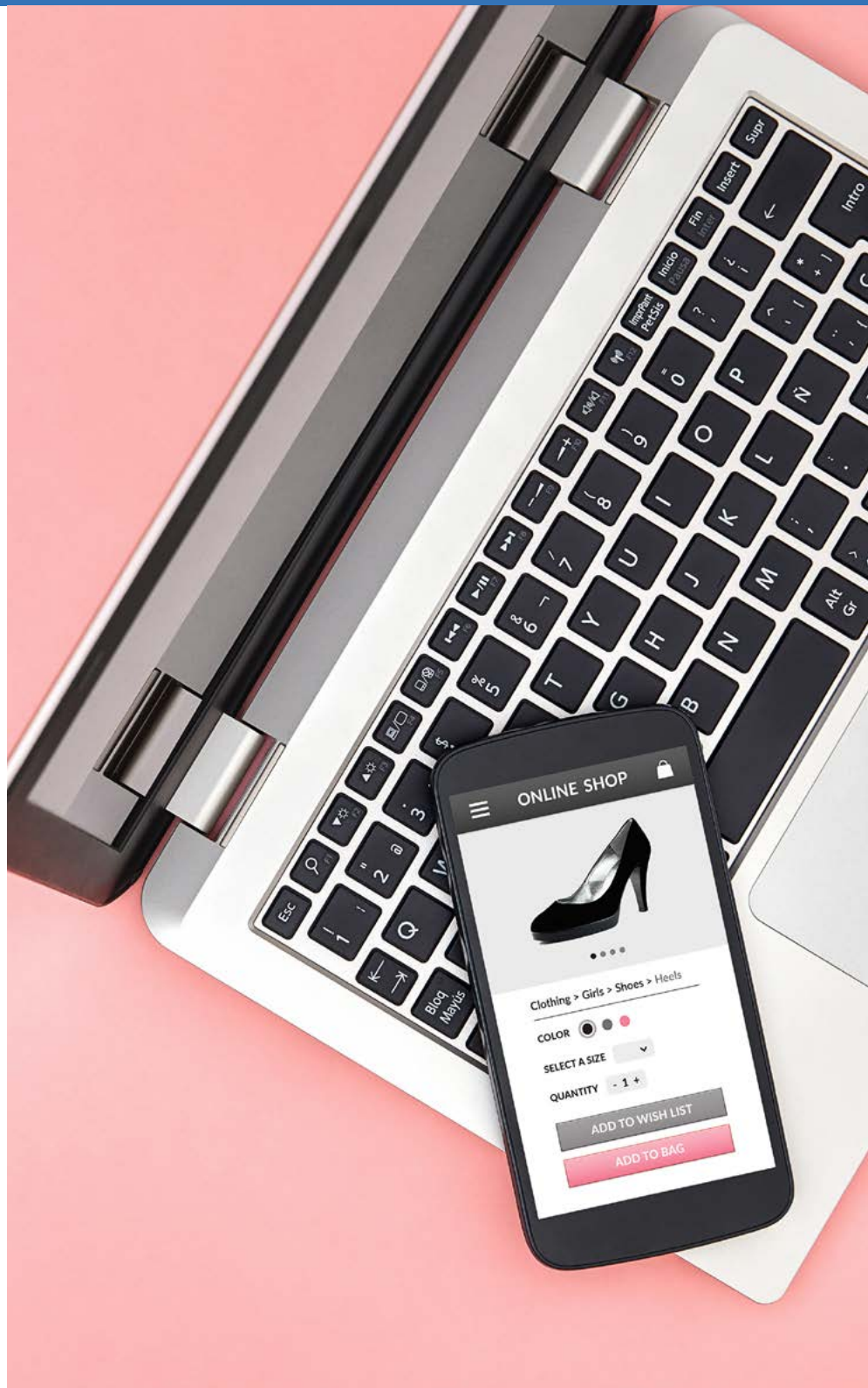
This year saw a **29% increase between H2 2018 - H2 2019**. This rise may be attributed to more fraudsters trying their luck against retailers with legacy systems in place and that are at higher risk for exploitation. It also reflects the repeat targeting of newer and more vulnerable areas of the customer journey, including loyalty programs or returns policies. These underprotected areas make for lucrative and alluring targets for repeat fraud.

The Way Forward

With rising consumer expectations and emerging vectors of fraud and abuse, merchants need to be prepared to better protect their businesses and customers. Amid growing sophistication in fraud attacks, contending with abusive behaviors perpetrated even by good customers, and balancing the need to offer more streamlined customer benefit offerings – merchants have their work cut out for them. In order to strike the right balance between fraud and abuse prevention, while ensuring a best-in-class customer experience, merchants require the right fraud prevention solution.

Legacy fraud stacks composed of multiple fraud tools or vendors that aim to solve different fraud and abuse pain points result in siloed fraud management efforts. These disparate tools may target one-off problems, but they ultimately result in costlier and less accurate fraud and abuse decisioning. Without sharing or leveraging data between vendors or tools, businesses are unable to build strategic solutions to their fraud and abuse problems. A rules-based approach is reactive, allowing fraudsters and opportunistic customers to stay one step ahead.

Instead, businesses need a single, comprehensive fraud prevention platform capable of assessing trust at every point of interaction in real time – from login, to coupon redemption, delivery, and post-purchase experiences.



A best-in-class solution will leverage data from across industries, enterprises, geographies, and fraud vectors, giving businesses the confidence to build deeper customer relationships and unlock the full promise of commerce based on trust.

Fraud attacks and abusive behaviors are growing more targeted and sophisticated. They require a more nuanced prevention system that is able to accurately distinguish legitimate customer behaviors (including coupon redemption or returns requests), from abuse and fraud. In partnership with a fraud prevention platform that leverages a robust global merchant network of data, merchants will have greater context into both fraudulent and legitimate customer behaviors, allowing more accurate fraud decisions to be made. A global merchant network leverages data and the online activities of millions of global users from across leading enterprises. This reveals insights, learnings, and linkages between users in the network to deliver higher accuracy in fraud decisions, even when a user appears in the network for the first time. The system amplifies and refines identity-linking capabilities. Enterprises should look for a fraud prevention partner that offers a unique combination of fraud expertise, identity linking technology, and a global network of data, to ensure that their business and customer accounts are protected from even the most sophisticated fraudsters and opportunistic abusers.

1. The Rising Tide of Loyalty Fraud - And How To Stop It
2. Coupon Fraud Is Crime, Event If It Feels Harmless: Coupon Counselor

Methodology

With over $150 billion in e-commerce transactions, the Eighth 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

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

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

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

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.

ABOUT FORTER

Forter is the leader in e-commerce fraud prevention, processing over $150 billion in online commerce transactions and protecting over 600 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 was recently named the Leader in e-Commerce Fraud Prevention by Frost & Sullivan.

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

Learn More at **www.forter.com**