



# How Online Fraudsters are Exploiting Omnichannel Retail

Understanding the spectrum of online risk

# Contents







- 03** Omnichannel Retail: Digital transformation vs. digital evolution
- 04** Real-World Risk: Retail fraud in action
- 07** Future-proofing your business starts with Digital Trust & Safety



Omnichannel retail fraud is a growing threat in a changing world. Merchants with brick-and-mortar roots face a digital-first future shaped by convenience, and targeted by tech-savvy fraudsters who are crawling out of every corner of the internet to take advantage of online consumers. With a global pandemic forcing shoppers and fraudsters alike to change how they operate, that future is rapidly becoming today's reality.

# Omnichannel Retail: Digital transformation vs. digital evolution

Many omnichannel retailers—merchants that sell goods online, in-store, and using various marketplaces—aren’t sure how to get started with online fraud prevention. Others have established their digital presence, and are ready to evolve their fraud strategies beyond too many rules and tools. We call these two groups Digital Transformers and Digital Scalers.

Digital Transformers	Digital Scalers
	
<p>Business is done primarily in physical stores, with a modest online presence</p>	<p>Business is primarily done online, with or without physical stores; may have robust mobile website or app</p>
	
<p>Physical and digital operations are not fully integrated; BOPIS (buy online, pick up in store) or delivery may be relatively new concepts</p>	<p>Hybrid physical and digital operations, with clear connections available on the customer journey (e.g., online order for pickup)</p>
	
<p>Friction is used at most or all steps of the customer journey (e.g., CAPTCHA), with a focus on loss prevention</p>	<p>Customer journey accelerators may be in place (e.g., one-click checkout), with a focus on speed</p>

Wherever a business is in its digital journey, all omnichannel retail merchants need to understand and address the external challenges they face, from legacy fraud tactics to emerging, more sophisticated vectors. Digital fraud evolves constantly, making it necessary for retailers to adapt how they fight it—both in-store and online.

# Real-World Risk: Omnichannel retail fraud in action

Omnichannel retailers are subject to the same types of fraud all merchants encounter—like stolen payment information, account takeover attempts/identity fraud, and promo abuse. And, because fraudsters are constantly evolving and improving their tactics, they’re able to tailor their attacks to specific verticals. The following are examples of ways fraudsters have altered well-known strategies to take advantage of omnichannel retailers.

## Promo abuse and payment fraud

1

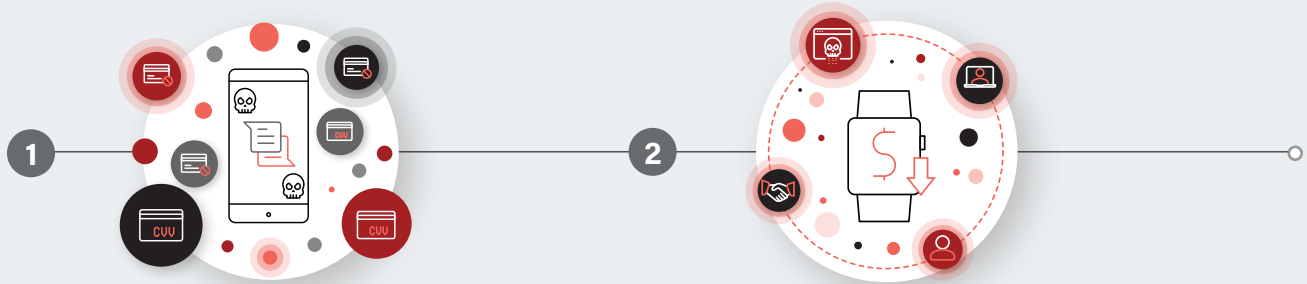
Using messaging apps and forums, professional fraudsters advertise their services—i.e., an ability to buy goods at heavily discounted rates. An opportunistic shopper responds, adds items to their shopping cart on a retail app, and sends a screenshot of that shopping cart to the professional fraudster via direct message.

2

Using stolen payment information, the professional fraudster buys the items. Then, they send a verification screenshot to the shopper, who finalizes the transaction by sending payment to the professional fraudster—usually in the form of cryptocurrency.



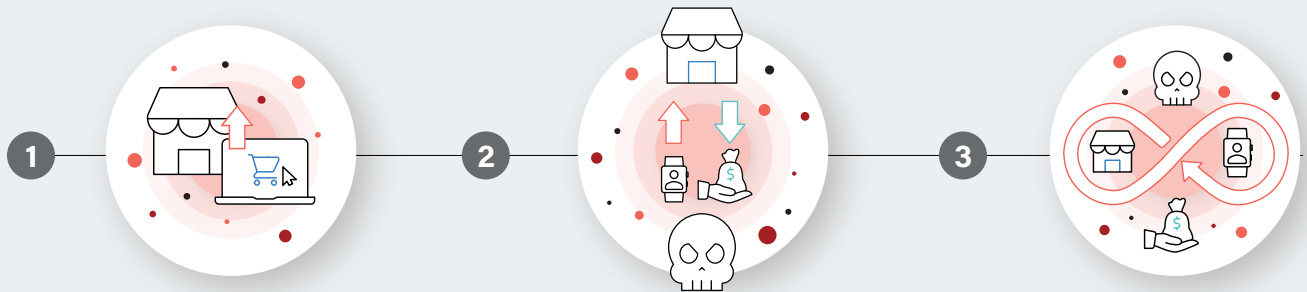
## Content fraud and card testing



By posting fake content listings on a two-way marketplace, fraudsters work together to test stolen payment information.

Several users with identical IP addresses create multiple listings at a specific price point; to test info, they “sell” the items to each other, after “haggling” those prices down to a minimal cost (\$1 USD). The listings are often uncharacteristic for the marketplace, purchased on the same day, and may include several fake reviews of the products listed to strengthen the appearance of authenticity. These types of fraud rings typically set up similar attacks across the internet.

## Buy online, steal in-store



One of the world’s premiere online marketplaces is now offering in-store returns at select retailers ([BORIS](#) - buy online, return in store), and fraudsters are taking advantage.

After purchasing an item via the online marketplace—likely with hijacked payment info—they’ll head to a physical retailer to “return” the item. The fraud could stop there, with the fraudster receiving store credit for the goods they bought online using stolen funds.

Some take it further. Instead of bringing in the item they “bought” online, they’ll grab that same item from the brick-and-mortar store’s showroom and execute the in-store return—walking away with both store credit worth that item’s value and the item itself.



## Non-refundable funds

1

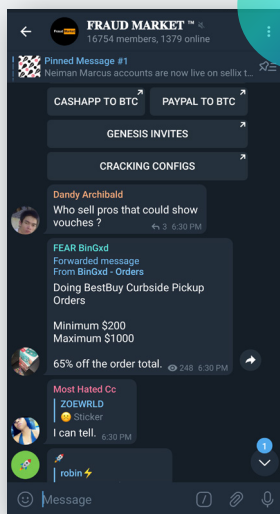
Refund fraud happens when fraudsters return legitimate, damaged, or illegally acquired goods with the hope of receiving money, store credit, or replacement (“free”) goods in exchange.

2

Fraudsters—typically a “refunder” and a “shopper”—link up on messaging forums. The shopper orders an item within a retailer’s stated guidelines. Once the item arrives, they contact the refunder and hand over proof of purchase.

3

These “refunders” know what will work on the companies they target, and which retailers will respond to claims that an item never arrived. Once a refund is provided to the cardholder by the retailer, the shopper then pays the refunder ~15-30% of the order value for their service.



It’s now more important than ever to be prepared for these types of attacks. The entire economy has seen unprecedented departures from typical consumer (and fraudster) behavior. Since the onset of the pandemic, the retail industry has shifted dramatically: U.S. retailers’ online year-over-year revenue growth **shot up 68% in mid-April 2020**, and Sift’s global network data showed a **70% increase in the average value of attempted fraudulent transactions** across all of e-commerce between October and November 2020.

# Future-proofing your business starts with Digital Trust & Safety

These dizzying surges in volume, and the fraud they inevitably attract, aren't just alarming for small businesses and local shops. During its 3<sup>rd</sup> quarter 2020 annual earnings call, retail giant Best Buy reported that **80% of its BOPIS orders** are ready in less than 30 minutes (on average), and **40% of its online sales** are coming from these types of "brick-and-click" transactions. That's a massive chunk of business being done both online and in person—with the current challenges of social distancing and mask mandates making customer identification difficult, if not impossible.

Finally, this mass migration to digital commerce won't be temporary. The pandemic may have forced retailers to get online or scale their e-commerce efforts faster than they'd planned, but even the long-awaited return to "normal" won't look like it once did. It's driving a permanent shift towards digital-first consumerism, making it imperative that merchants understand both how complex the **e-commerce fraud ecosystem** really is, and the types of retail-specific digital fraud that they're up against.

With Sift's Digital Trust & Safety Assessment, omnichannel retail merchants can get expert advice from our team of Trust and Safety Architects. They'll help you take stock of current fraud prevention and tech challenges, discover how to best protect consumers while delivering standout experiences, and unearth new possibilities for rapid growth.

[TAKE YOUR ASSESSMENT TODAY](#)



The economic impact of the pandemic has made fraud a lot more appealing. Recent reports have shown an increase in friendly fraud, and that's no coincidence. Consumers may falsely file a dispute with their credit card companies in order to recoup the funds for a purchase they received and intend to keep.

**JANE LEE**

Trust and Safety Architect, [Sift](#)

## End-to-end intelligent automation with Sift

Sift is the leader in Digital Trust & Safety, empowering companies of every size to unlock new revenue without risk. Our cutting-edge platform dynamically prevents all types of online fraud and abuse with intelligent automation that adapts based on Sift's unrivaled global data network of 70 billion events per month. Global brands including Twitter, DoorDash, and Wayfair rely on Sift to catalyze growth and stop fraud before it starts.

Visit us at [sift.com](https://sift.com) and follow us on [LinkedIn](#).