

RETAIL

Omnichannel retail gives fraudsters more opportunities

March 18, 2019



Online fraud within luxury retail is becoming more prominent. Image credit: Saks Fifth Avenue

By SARAH RAMIREZ

Rates of fraud on jewelry and luxury goods were up nearly 20 percent in 2018, as the high sticker value on these items makes these illegal activities more lucrative.

Subscribe to **Luxury Daily**
Plus: Just released
State of Luxury 2019 **Save \$246 ▶**

According to Forter's Q1 2019 [Fraud Attack Index](#), ecommerce platforms are also seeing an increase in fraudulent attacks. With criminals turning to more automated methods of attack, online retailers are especially vulnerable.

"The luxury industry is a popular target amongst fraudsters because high-ticket items lead to a more substantial payout," said Michael Reitblat, CEO and cofounder at [Forter](#), New York. "A lot of luxury brands are exploring the omnichannel retail space, but unfortunately, along with the expectation of increased revenue this strategy also exposes them to more opportunity for suspicious activities."

Online loopholes

Despite luxury and jewelry companies' attempts to protect themselves from criminal activity, fraud attacks grew 19 percent from the fourth quarter of 2017 to the same period in 2018.

Luxury goods become even more desirable targets during the holiday season and other peak shopping times. Christian Louboutin and Balenciaga saw double the number of attempted attacks during the 2018 holiday season ([see story](#)).



Rates of fraud on jewelry and luxury goods were up nearly 20 percent. Image credit: Chopard

As luxury retailers introduce more flexibility in shopping options, such as click-and-collect, there are also more opportunities for criminals.

"Click-and-collect' fraud is an increasingly popular scam where fraudsters use stolen personal information to buy online and collect their order in store, no shipping address necessary," Mr. Reitblat said. "This form of fraud makes it easy for fraudsters to fly under the radar, providing them with a discreet location to pick up their stolen goods that can't easily be traced back to them."

Additionally, the apparel and accessories sector experienced a 47 percent increase in fraud attacks year-over-year.

Clothing is relatively easy to resell, and bulk purchases are not flagged as suspicious with the same frequency as other items. Shoppers are also more accustomed to buying apparel from third-party platforms, giving fraudsters more opportunities.

Limited-edition pieces, particularly footwear, are popular targets for criminals. Exclusive items are more likely to find eager buyers, so fraudsters turn to bots to help acquire new releases online.

The travel industry is seeing different patterns of fraud.



Land travel saw fraud attacks increase 19 percent. Image credit: Marriott International

Air travel saw fraud attacks decrease by 29 percent in 2018, although major airlines were attacked 37 percent more than low-cost carriers. Land travel and accommodation services, however, saw a 19 percent increase in fraud.

As hospitality brands look to streamline their online processes to improve the customer experience, they are also limiting red-tape measures such as proof of identity. These simplified online transactions then become more vulnerable to attacks.

Closer look

Affluent consumers are also victims of fraud, making it an issue that is not limited to retailers.

Nearly half of shoppers in the United States have dealt with credit card fraud, with many victims not returning to the retailer after the incident, leaving merchants in a precarious position.

Credit card fraud has varying repercussions for retailers, who have to pay for the cost of the fraud and also see a damaged reputation and revenue loss. However, fear of fraud has also led to 30 percent of consumers having

legitimate purchases declined, again negatively impacting the relationship between shoppers and retailers ([see story](#)).

Hospitality brand Marriott continues to deal with the fallout of a security breach for its Starwood Hotels.

Starwood's reservation system recently saw a security hit in which guests' passport information and payment cards were compromised. While the hospitality group previously announced that the incident involved up to 500 million guests, further investigation has led Marriott to believe that only 383 million customers had their information stolen ([see story](#)).

"It's actually pretty common for data exposed in cyber attacks to be stockpiled for future use," Forter's Mr. Reitblat said. "It was three or four years before Forter started to see the information stolen in the eBay hack of 2014 and LinkedIn's 2012 leak used to commit ecommerce fraud.

"Similarly, we've seen little use of the Equifax or Marriott data," he said. "These are two of the worst breaches that the retail identity space has ever seen because, aside from their massive scale, high-quality information like social security numbers and passport details were compromised.

"This data is particularly valuable because unlike passwords and email address it can't be changed, so online criminals can use it to commit full-fledged identity theft."

© 2020 Napean LLC. All rights reserved.

Luxury Daily is published each business day. Thank you for reading us. Your [feedback](#) is welcome.