Luxury Daily®

The News and Intelligence You Need on Luxury

RETAIL

Luxury goods' high risk, high reward attract fraud: report

March 8, 2017

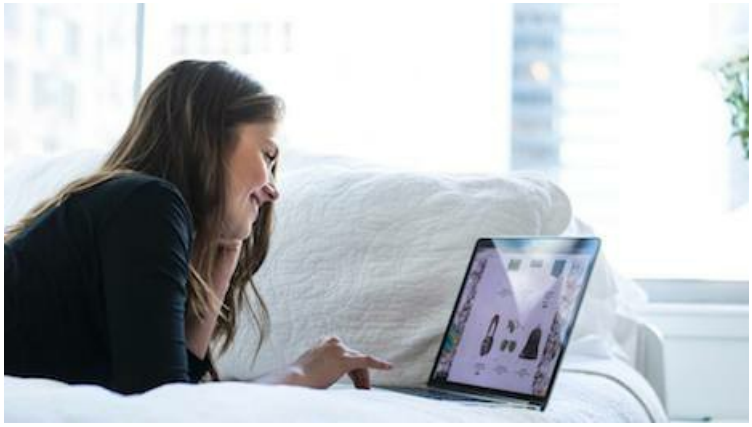

Image courtesy of Saks Fifth Avenue

By SARAH JONES

The rate of fraudulent transactions in the luxury goods category declined 8.4 percent in 2016, but the industry remains one of the hardest hit, according to a new report from Forter.

It may be more difficult to have a high value order approved, but if fraudsters manage to get through, luxury goods are easy to move and fetch appealing resale prices. The increasingly sophisticated attackers are not deterred by a failed attempt, making it necessary for luxury brands to maintain vigilant.

"Luxury goods are still enormously popular with fraudsters," said Michael Reitblat, CEO and co-founder at Forter. "Sadly, luxury retailers certainly can't relax their caution.

"However, the fact that so many luxury retailers have become aware of the dangers of fraud in recent years, and have taken steps to deal with it and protect their businesses, meant that fraudsters started thinking of ways around these defenses," he said.

"One notable tactic was attacking the same or very similar goods through apparel sites instead of luxury ones, because in general apparel sites, which have traditionally been less of a target, are less hyper-aware of this threat and less well-equipped to deal with it as a result. So rather than going for a Michael Kors bag on a luxury site they went for the same bag or an equivalent on an apparel site, where it is one of the more expensive items on offer."

Forter's Fraud Attack Index, conducted along with the Merchant Risk Council, measures the fraud attempts on U.S. merchants, looking at the percentage of dollars that were tied to fraudulent orders reported. For the purposes of Forter's report, luxury goods are defined as apparel, accessories and jewelry.

Continued threat

Following the roll-out of microchip readers at most points of sale in the United States, fraudulent credit card present transactions became more difficult. Those looking to commit credit card fraud moved their activities online.

Digital channels have also made the job easier for would-be fraudsters to enter the field. They can get their hands on customer data stolen during breaches and enter it into ecommerce sites.

Mobile security risks remain a serious concern for marketers and consumers alike now that a new report has shown

that more than 200 different mobile applications and Web sites were leaking personally identifiable information over the course of the last year.

The data comes from a new report on data security from Wandera. The report studied mobile apps and sites from 20 different countries and found significant evidence of leaked information (see story).

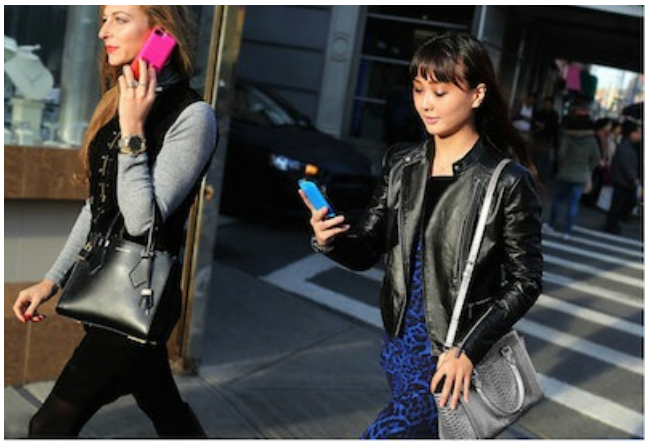

Image source Michael Kors

Following a surge in attacks in late 2015, fraud across industries increased 8.9 percent in 2016. Within the United States, this fraudulent activity spiked during the holiday season.

While the so-called fraud tsunami of 2015 appears to have calmed down, online businesses are still at a 2.5 greater risk of attack than domestic retailers. In addition, international transactions are 63 percent riskier than those within a home market.

"In part, it's just a question of numbers - there are a lot more fraudsters outside the U.S. than inside," Mr. Reitblat said. "The rest of the world is very big, and there are some fraudster hotspots in both developing countries and Eastern European ones in particular.

"As well, fraudsters love to target U.S. sites for their attractive merchandise, even if that means dealing with international shipping challenges. That challenge isn't really much greater than a U.S. fraudster targeting a state on the other side of the country.

"It's important to highlight here that this doesn't mean that retailers should avoid cross-border commerce. On the contrary in fact, the Fraud Attack Index found a decrease in international fraud rate, attributed to the increase in international orders. There's great business in selling overseas, you just have to do it with due care and preparation."

Luxury goods are one of the most popular targets for cross-border fraud. Early numbers for the first quarter show that $14.2 of every $100 are at risk, and at a high point, there were three times the rate of international fraud as there were domestic instances.

Image source Louis Vuitton

"Luxury retailers need to be aware that the behavior of consumers in different countries varies widely, and their fraud prevention needs to be sensitive to that fact," Mr. Reitblat said. "If you try to treat Australian customers exactly like U.S. ones, you'll turn away good ones and let through fraudsters.

"Your fraud prevention system needs to be aware of the differences and analyze customers accordingly," he said. "One element behind this. Keep analyzing your customer data, all the time, from numerous different angles. That's

the only way you can know how the differences play out in your industry and on your site, and protect yourself accordingly."

In general, $5.91 out of every $100 spent with luxury merchants are at risk for fraud, making these high-ticket goods more popular than most other physical products.

One trend that Forter has seen is criminals targeting more mid-range luxury goods. Slightly lower priced merchandise is less apt to arouse suspicion, and there is a large market for these more budget-friendly goods in resale.

One step ahead

Merchants and frausters play a cat and mouse game, with those that have been thwarted typically moving on to a new target or a new method to get ahead of retailer blocks. More secure payment methods present a challenge, but these individuals will search for a weakness and exploit it until it is reinforced.

A growing technique deployed by fraudsters is account takeover, in which they will login to a customer's account, either on a retailer's Web site or payment services such as PayPal or ApplePay, and then use it to make purchases. These are less likely to raise flags due to built-in authentication information.

Third-party payment platforms have seen an increase in fraud, while retailer account takeovers have declined lately.

Financial institutions Mastercard and Visa have banded together to make mobile and digital payments safer on either of their mobile pay platforms in an effort for wide spread adoption.

While mobile pay is starting to flourish, fraud is still a major point of concern for consumers. Visa and Mastercard, both of which have their own mobile pay platforms, will now allow requested tokenized credentials from each other to be used in their respective platforms instead of credit card information (see story).

Mastercard's Masterpass

"The nature of fraudsters is that they are highly creative and fast moving," Mr. Reitblat said. "What works against them today might not work anymore tomorrow if they've found a way around it.

"That being the case, the main thing for luxury retailers to be aware of is that they have to stay on top of their data, and the trends in the fraudster ecosystem," he said. "It's vital to know what your customers are doing, both good and bad, and what fraudsters are doing, if you are going to protect your site effectively.

"This is a challenge for many retailers who rely heavily on manual reviews. Most of the time of the fraud department is taken up with reviewing transactions manually rather than assessing trends and patterns, and devising new ways to identify and block fraudsters.

"Retailers need to move away from this kind of setup. Increased automation, or full automation, of fraud prevention for individual transactions can remove the burden of manual reviews and enable retailers to take a proactive rather than fully reactive approach to fighting fraud."