Balancing Fraud Protection and Frictionless Checkout

Retailers attempt to improve customer experience without increasing exposure to cyberthreats

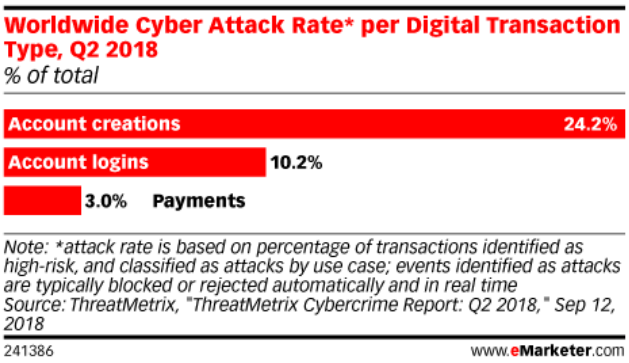
ARTICLE

Rimma Kats

As an industry, retail is one of the most vulnerable to cybercrime. Ecommerce transactions can provide a wealth of fodder for fraudsters, including personal information and credit card details.

According to a Q2 2018 ThreatMatrix report, ecommerce companies using its digital identity network experienced 91 million attacks, which is business as usual as the figure was consistent with the same period last year.

The types of cybercrime, however, are changing. An attack rate of 24.2% means nearly one in four new accounts created on ecommerce sites in Q2 2018 were fraudulent, a 130% increase year over year. Account login fraud using stolen credentials was the second-most common attack (10.2%) while using stolen payment credentials made up 3.0% of total attacks.



Account login fraud, which some call "takeover" fraud, tripled last year, according to Javelin Strategy & Research, costing $5.1 billion in the US.

An interesting side-effect of cross-border ecommerce's growing popularity—more than half (54%) of transactions on the ThreatMatrix network are cross-border—is that it has raised retailers' guard in accepting sales from countries and buyers perceived as high-risk. Because of stricter rules, cross-border transactions are 69% more likely to be rejected than domestic ones.

These fears aren't unfounded, though. Digital cross-border traffic has a 22% higher likelihood of identity spoofing and 15% higher risk of device spoofing.

Reducing friction at checkout—one way digital retailers are trying to improve the customer experience—is often at odds with cybercrime protection. This is especially true with mobile commerce.

In a November 2017 survey by Internet Retailer and ACI Worldwide, 20% of retailers said that fraud prevention was most important, 26% said fraud prevention was more important but they had an eye on the frictionless experience while 22% were trying to find a compromise. Only 6% considered ease of transactions a priority over protecting from cyber threats.