

Retailers set to lose billions as card-not-present fraud rises

Retailers stand to lose \$71 billion globally from fraudulent CNP (Card-Not-Present) transactions over the next five years, according to new data from Juniper Research. The data found that a number of factors, such as the USA's shift to EMV cards, delays in 3DS 2.0 (3D-Secure) and click-and-collect fraud were key drivers behind the rise.



©Sergey Rasulov via [123RF](#)

The company's latest research, *Online Payment Fraud: Emerging Threats, Key Vertical Strategies & Market Forecasts 2017-2022*, found that many merchants still perceive combatting fraud as too expensive. Consequently, they have been ill-prepared to deal with the shift to online fraud following the introduction of EMV (CHIP and signature) payment cards in the USA.

Nevertheless, cost analysis of FDP (fraud detection and prevention) solutions found that in most instances, merchants would receive value from their investment. The analyst house, therefore, urged players across the value chain to increase their efforts in educating merchants on the benefits of FDP.

Physical goods a key target

Additionally, the research forecast that fraudulent CNP physical goods sales will reach \$14.8 billion annually in 2022. It argued that click-and-collect services were particularly vulnerable given the lack of a residential delivery address. Meanwhile, retailers are reluctant to impose rigorous ID checks on pick-up for fear of damaging the consumer experience and reducing conversion rates.

Building higher walls

The research predicted that three key battlegrounds would emerge in the fight against fraud in 2018. It cited machine learning as a key tool in identifying genuine users, while the shift to mobile e-commerce would rely on 3DS 2.0 and biometrics.

“2018 will herald the arrival of new tools in the fight against fraud”, noted research author Steffen Sorrell. “3DS 2.0 will finally begin to rollout and will mark a paradigm shift in terms of merchants and issuers leveraging shared data. We also expect passive biometrics, such as the manner in which a device is handled, to become key in the future.”

The whitepaper, *Future Fraud: 3 Key Battlegrounds in 2018*, is [available to download](#) from the Juniper website together with further details of the full research.

For more, visit: <https://www.bizcommunity.com>