Online Fraud Detection on 5 ecommerce fraud predictions for 2017

Ecommerce fraud is on the rise as more consumers turn to online shopping. Luckily, by being vigilant, merchants can fight fraud and win.

As the number of consumers turning to online shopping increases, the rise of online fraud is also rising.

Those committing internet crimes are depriving their victims of either funds, interests, personal property and/or sensitive data. As the threat escalates, consumers and companies alike are seeking various methods to tackle the phenomenon.

Ecommerce fraud has a long and controversial history. Thus, providing a forecast for the months ahead can help retailers adopt an adequate solution to confront the many challenges in 2017.

1. **Identity theft and friendly fraud**

The main threat will remain identity theft. Fraudsters will seek your personal information. Their main goal is to use a different identity and, for example, place an online order. Identity theft also includes a concept known as man-in-the-middle attacks where credit-card data is intercepted and copied as it is transferred online.

In the practice of friendly fraud, a customer pays for ordered goods and/or services through a direct debit or a credit card. The second step involves a deliberate chargeback from the issuing bank, taking place only after receiving the purchased goods or service. The involved fraudster then goes on to claim the credit card or details of customer's account has been stolen. While the "customer" is reimbursed, they decide to keep hold of the goods.

2. **Merchant and triangulation fraud**

In merchant fraud, the goods are provided at extremely low prices yet no shipment takes place. There is also a wholesale version of this fraud. No specific method enjoys any exclusivity, yet it is common knowledge that no-chargeback payment methods come to life in this practice of fraud. This also involves a majority of the push payment types.

Considered as one of the more complex ecommerce attack methods, triangulation fraud involves quite a bit of collaboration, as three points are involved. Role #1 belongs to an ordinary customer placing an order through a type of credit, debit or PayPal tender. Role #2 involves a fraudulent seller receiving the placed order, then requesting the actual product from a legitimate ecommerce website while using a stolen credit card. Role #3 is the part played by a legitimate ecommerce website completing the order requested, completely unaware of the criminal nature.

3. **Affiliate and clean fraud**

Two types of affiliate fraud are popular these days, while both seek one objective. By manipulating sign-up data or traffic, fraudsters are pursuing the objective of collecting more money. Options include actual people using fake accounts who log into sites of merchants or simply employing an automated process.

Clean fraud also involves the use of a stolen credit to make an order. In such a method, criminals resort to complicated practices, such as using sound analyses equipped in fraud detection systems, and obtaining in-depth data on the owners of stolen credit cards. This information is needed to deceive the payment process and bypass the fraud detection solution.

4. **The counterattack**

Online piracy and the sale of counterfeit goods will face new challenges, as the U.S. Department of Justice has declared a new initiative teaming up state and local law enforcement agencies in this struggle. Washington has already pumped $3.2 million into this campaign.

New state-of-the-art advances are also making life more difficult for fraudsters, especially with the introduction of EMV chip card technology. This is a significant leap forward in enhancing credit card security, providing a strong incentive for small and large companies to jump on the bandwagon.

5. **Fighting fraud**

Fraud prevention and chargeback guarantee for ecommerce merchants, Riskified works on establishing genuine financial security between online customers and ecommerce merchants. This company delivers ecommerce fraud prevention solutions for merchants to certify previously avoided transactions.

At a time when the relationship between a buyer and a seller is in search of trust more than ever before, customer experience and the bottom line is protected through the services provided by this firm in pioneering the charge-back guarantee.

“We founded Riskified with the retailer in mind and have grown adept at servicing the needs global retailers have as they expand their e-commerce and m-commerce operations to provide more personalization to consumers,” says co-founder and CEO Eido Gal, signaling the high demand and importance of such services in today’s digitized world.

As calls for digital goods increase, we are witnessing a rise in the necessity of protection against fraud.

“Digital goods, such as electronic gift cards and e-tickets, are becoming increasingly popular. In the U.S., over $127 billion is spent on gift cards annually,” Shalhevet Zohar explained in a blog post about ecommerce fraud trends.

Such statistics, growing as we speak, demonstrate the huge market fraudsters seek to tap into—and the utmost necessity for consumers to be adequately prepared.

Final thoughts

The fraud landscape is a constantly changing and evolving phenomenon, demanding an adaptive approach to remain at top of your game. Retailers in the U.S. have suffered $109 billion more due to suspected fraud costs resulting from false declines of legitimate orders. This is far beyond actual fraud losses. The ecommerce industry is increasing its demand for fraud prevention platforms, and there is a new revenue opportunity for those companies able to provide such high-valued expertise.