Relying on Blacklists for Fraud Prevention? You Risk Losing Your Customers

Lynn White April 26, 2018

Blacklists are not universally effective, and ecommerce merchants risk losing customers if they use them. The following explains why blacklists can be costly to your business.

(Newswire.net -- April 26, 2018) -- Using extensive blacklists was once seen as an effective way to prevent fraud. Doing so involved checking each transaction against a list of known-bad credit card numbers, phone numbers, and IP addresses in an attempt to weed out fraudsters based on their transaction history. Yet blacklists are not universally effective, and ecommerce merchants risk losing customers if they persist in using such a blunt instrument. Below we'll explain why blacklists can be costly to your business, and what the alternatives are.

Blacklists and false declines: a costly mix

Protecting against ecommerce fraud comes down to testing the parameters of a transaction against a set of rules, and a corresponding data set. Sophisticated ecommerce fraud protection systems will use a mix of established rules, dynamic machine learning and frequently updated data sets. On the flipside, older and less advanced systems will simply evaluate transactions against a blacklist.

The problem with relying on a blacklist alone is two-fold. First, fraudulent actors who are not yet blacklisted will not be caught. Second, blacklists can lead to false positives, where bona fide transactions are declined when they shouldn't be. This is highly costly for businesses, with false positives leading to an estimated $8.6bn lost to US ecommerce vendors in 2016 alone.

Operating fraud prevention on the basis of blacklists result in false positives because blacklist data tend to become stale quickly, and due to their blunt nature. The "owners" of blacklist data points such as telephone numbers and IP addresses can change, so merely blocking on that basis can easily lead to blocking an honest shopper. Data points can also reflect multiple individuals, with some physical addresses linked to multiple occupants or a group of people sharing a single IP address.

Ecommerce merchants need to think through the costs of blacklist-associated false positives. It's not only the revenue loss behind individual transactions that are a concern, but customers may feel a merchant is telling them that they're simply not interested in their business. Though some customers may come back at a later time, many may move on to competitors and never make use of the store in question in the future. This could present a large revenue loss, all on the basis of a false positive.

Moving on from blacklists and false positives

The nature of blacklists combined with the more advanced tactics used by perpetrators has led many ecommerce firms to adopt more advanced fraud monitoring solutions. Perhaps the most important principle ecommerce businesses should adopt is to never decline a transaction based on a single data point alone. Instead, multiple data points should be evaluated and only if a statistically significant number of red flags are raised should a transaction be halted altogether.

However, it is also important to move away from simply evaluating static data points. Instead, fraud protection systems should incorporate dynamic data points to weed out fraudsters. Data points such as credit card address verification systems (AVS), device identifiers and so forth are all useful but more dynamic data can provide far more insight into whether a user is authentic.

Dynamics factors are driven by an understanding of your user, including the way that the user browses through your site, their purchase history and the way they use a device. Automated fraud, in particular, will quickly raise red flags when judged against behavioral characteristics such as typing speed and browsing habits.

Finally, the dynamic aspect of fraud prevention also involves continuous learning. Fraud protection systems which can automatically build on the knowledge gained through experience is much preferred over those that need to manually adjust rules whenever the fraud landscape changes. Machine learning-enabled systems can help your business decline fraudulent transactions based on bleeding-edge knowledge, while at the same time avoiding the costly expense of false positives.

Don’t throw blacklists out altogether

This is not to say that blacklists are of no use. Parameters that indicate a history of fraudulent behavior, such as a known bad IP address, should be used in the fraud detection mix, but only as part of broader criteria. Advanced systems can algorithmically evaluate a large number of parameters to make an approve vs. decline decision and classic blacklist information can prove to be informative. The key lies in deploying blacklist data as one component of an advanced fraud protection system, not as the sole protective measure.

Source: http://newswire.net/newsroom/blog-post/00101447-relying-on-blacklists-for-fraud-prevention-you-risk-losing-your-customers.html