Guide to Reducing False Declines

modo

As the eCommerce industry continues to grow, customers are moving their activity online and relying more than ever on card not present (CNP) transactions to purchase goods and services. This, coupled with the United States' transition from magnetic stripe cards to chip cards, has resulted in an aggressive move by fraudsters from point of sale to online and mobile marketplaces. As an eCommerce merchant operating online, this isn't exactly the cherry you hoped would top your digital sundae.

False Decline Trends in eCommerce

6.67%

CNP Fraud

Expected to affect 6.67% of consumers by 2022, up from 3.97% in 2017.

51%

Risk of Attrition

51% of cardholders declined for an online purchase will decrease patronage of a merchant.

53%

Declined are Affluents

False declines online are more likely to affect the affluent. 53% of declined cardholders make more than $100,000 annually.

15%

Decline Rates

Decline rates of digital merchants average well above 15%.

1.79M

Compromised Accounts

In 2017, 1.79 million online merchant accounts were compromised, up from 530k in 2016.

Steps to Reducing False Declines

(while minimizing friction)

1 **Reduce Friction with the Use of Invisible Authenticators:** Start by using invisible authenticators to assess the behavior, device, and location of each user. Good customers won’t be pestered with unnecessary authentication measures, they won’t be wrongly identified as suspicious, and their transaction is less likely to be declined. That’s what we like to call a win-win-win.

2 **Block Bots and Fraudsters via Behavioral Analytics:** If you haven’t already, start blocking bots and fraudsters with some BA tactics. We’re talking, of course, about behavioral analytics. BA can evaluate how a user navigates through your site or app and more accurately identify malicious users. It can recognize when a user is suspiciously familiar with a page, which is a fraudster red flag alert that can mean bots are being used to make multiple fraudulent purchases.

3 **Verify Legitimate Users through Behavioral Biometrics:** Next up in your merchant arsenal of fraudster combat tools? Behaviometrics. These assess how a user interacts with input devices like the keyboard, touchscreen or mouse. By memorizing user cues, behavioral biometrics can confirm whether the individual is the same person who made purchases on the site in the past. Because yes, they did buy that cosplay outfit for ComiCon. They know it, and thanks to behaviometrics, you know it too.

4 **Minimize Friction with Risk-Based Authentication:** Artificial intelligence and machine learning tools aren’t just for Bond anymore. Today, you can use them to identify and assess the risk of every user in real time. Depending on the level of detected risk, how adept your authentication platform is, and the capabilities of the user’s device, certain step-up challenges can be strategically deployed without excessive friction. A simple “tap to approve” function is one example.

5 **Solve False Declines from the Issuer:** As a merchant, there are many things you can do on your end to stop false declines from occurring. But it’s a different story at the issuer level. You may think all your fraud tools go to waste when you get a decline from an issuer, but there are companies helping combat this. Mitigate the risk of customers getting falsely declined by looking for a company that offers multi-routing capabilities. When one processor declines a good customer, the transaction is automatically routed to another processor—and another, and another—until the payment is successful. A good customer gets their goods, and you get assurance that your customers are happy.