Card Testing Fraud

Often around Black Friday, cyber criminals like to test batches of stolen or compromised credit cards they have obtained. This is called Card Testing Fraud. These credit cards are NOT related to Jlive users, they are just random credit cards from around the world. But they may decide to use Jlive to see if the cards work.

Jlive is in the process of very soon releasing several precautions to block this behavior moving forward including adding CAPTCHA, browser fingerprinting, IP-based restrictions and more. In summary, we are on top of it.

Read more about Card Testing Fraud

Card testing fraud, a prevalent form of **credit card fraud**, is when fraudulent actors validate the usability of stolen **credit card** numbers. This fraud usually involves executing several low-value transactions on various websites. These small transactions are often unnoticed by cardholders and fraud detection systems, which tend to focus on larger, more irregular spending patterns. Those committing the fraud use these test transactions to verify the card is still active and has not been flagged or canceled because of theft and to confirm the card has a sufficient credit limit for purchases.

This kind of fraud uses legitimate transaction processes to prevent detection. Fraudulent actors often target websites known for processing a high volume of low-value transactions because those are less likely to trigger alerts. Once a card passes this initial “testing” phase and is deemed active and unblocked, its value to the fraudulent actor drastically increases. They might then use the card themselves to make more substantial purchases, or they might sell the card details on the illegal market.