The Holiday Shopping Season: A Prime Opportunity for Triangulation Fraud

As e-commerce sales increase, so does the risk of hard-to-detect online fraud.

As with everything else in 2020, this year's holiday season will be unlike any other. Public health authorities are warning that crowded malls and shopping centers pose a high risk for exposure to COVID-19 and are advising caution. We experienced a swift shift to digital channels in every sphere this year, and nowhere has that been more impactful than e-commerce. Demonstrating this point, Deloitte forecasts that holiday e-commerce sales will grow by 25% to 35%, or between $182 billion and $196 billion, over 2019's figures.

While online shopping reduces consumers' risk of contracting COVID-19, it introduces another danger: the increased risk of falling victim to online fraud. If predictions ring true, the volume of transactions will grow, making it easier for cybercriminals to hide and perpetuate fraud.

The risk of e-commerce-related fraud stems from several problems:

- Companies often do not know the entirety of their attack surface.
- Each entry point may require a different type of protection, which can be challenging from a resource perspective.
- Users' cyber hygiene remains a problem (e.g., reusing username and password combinations).
- Fraud is becoming more and more sophisticated.

The last point is notable. Even if companies know every entry point into their infrastructure and have airtight security and perfectly secure users, the evolving sophistication of fraud remains a fundamental issue. Predicting the next iteration of attacks is "often too little too late" — where the threat is found only after accounts are hijacked, money is withdrawn from bank accounts, and gift card values are stripped. This is because too many security vendors rely on detection-first technology.

How Triangulation Fraud Escapes Cyber Defenses

In the retail industry, triangulation fraud is a prime example of cybercriminals escaping detection despite robust cybersecurity measures in place.

A triangulation fraud scheme begins when a fraudulent seller posts an enticing below-market-price item, often on an online auction or marketplace. An unsuspecting customer places an order for the item and pays for it using a legitimate credit/debit card or other online payment tender. The fraudulent seller then uses stolen credit card credentials to purchase the product through a legitimate e-commerce website and ships it to the customer.

In the end, the customer receives the product, the fraudulent seller collects the payment, and the victimized credit card holder gets stuck with the bill. This makes the scheme hard to detect until the credit card holder disputes the charges as a fraudulent transaction. Because humans with legitimate credentials and payment details are involved in every step of the three-way transaction, defense measures can't stop the fraud because they don't detect it.

How to Stop Triangulation Fraud

If retailers want to reduce and mitigate triangulation fraud, they should start at the login page since the common denominator in these attacks is stolen credentials. While bots are not the main perpetrator of triangulation fraud, bots do allow criminals to complete transactions at a scale that makes them highly profitable.

Credential cracking and related attacks are simplistic bot attacks that act as a springboard to more sophisticated fraud, including triangulation. Conventional security wisdom would suggest adding CAPTCHA or multifactor authentication to the login page to deter bots, but we know that fraudulent credentials are widely available on the Dark Web, and bots can easily bypass CAPTCHAs using tools like DeathbyCaptcha.

To mitigate these sophisticated schemes, retailers must be able to judge user legitimacy in real-time. For example, on a computer, does the user type too quickly to be human? Is the mobile device real or a device emulator?

These kinds of biometrics, along with hundreds of additional network signals and device profiles, provide the data needed to determine who or what is behind a transaction. And this insight enables businesses to fingerprint users and track their behavior once inside accounts. If the same fingerprinted user begins logging into dozens, hundreds, or even more legitimate accounts but then drops off, there is a high likelihood there's a bot behind the logins. The company must freeze the accounts before the bot can hand the scheme off to a human to complete a manual attack. Only then can we cut off inroads before these schemes proliferate.