Holiday Shopping Threats

Triangulation Fraud

Prepared by:

FS-ISAC's Triangulation Fraud Working Group
Communications and Awareness Subgroup

Holiday Shopping Threats

Triangulation Fraud

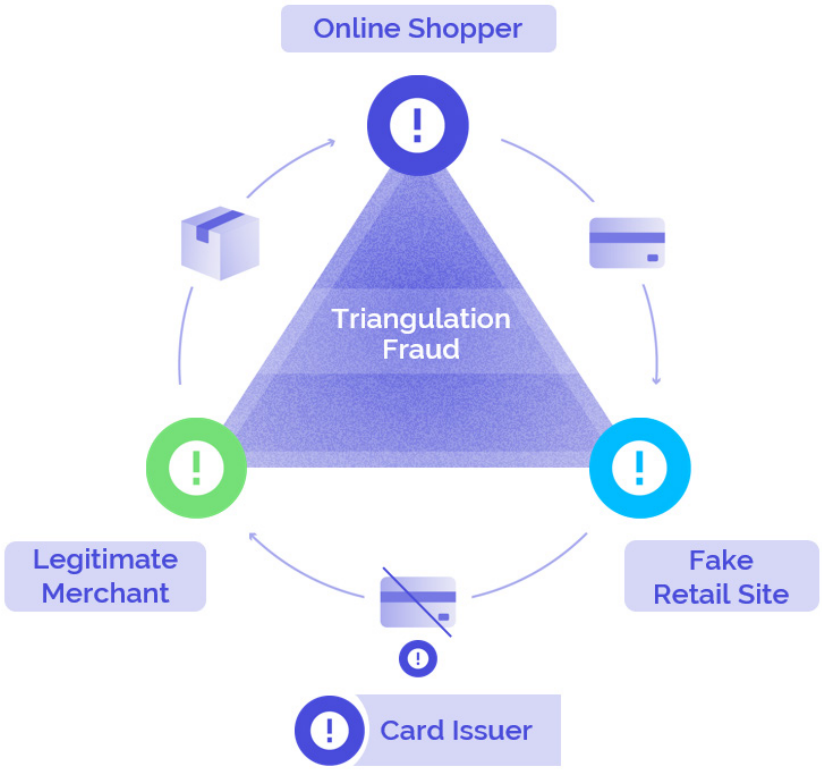
Overview

Triangulation fraud has many victims, including online shoppers, card-issuing financial institutions, merchants – even the employees of the fraudster. Moreover, triangulation fraud costs millions of dollars, harms consumer trust, and damages the brand reputations that financial institutions and merchants rely upon to drive their businesses.

Triangulation fraud is also a demonstration of the impressive collaboration that criminal groups can achieve. To get and stay ahead of fraudsters, financial institutions and merchants must share insights on these crimes. Strong cross-sector, public/private collaboration is critical to making the "job" of the criminals so difficult that it undermines their operations' ROI, forcing them to a new business model.

Triangulation Fraud is Clever and Hard to Detect

The scheme is called 'triangulation fraud' because it brings online shoppers, a fake retail site, and a legitimate merchant together in a fraud triangle. This is how it works:



- An online shopper sees a big discount on an item at what appears to be a legitimate retail website and places an order.
- In actuality, the website is operated by a criminal ring, which uses card credentials stolen from another shopper to order the item from a legitimate merchant's site.
- The legitimate merchant completes validation, which the criminals creatively deceive, and fulfills the order.

- The online shopper receives the item, unaware that the criminal ring has stolen their payment details and will use them in future fraudulent transactions – just as they did to the person whose payment information they stole to place the order.
- The shopper is so happy with their discounted product that they might accept the request to provide a positive review, perpetuating the scam.

Beware!

Triangulation fraud first erupted during the Black Friday holiday sales in 2022. Having targeted large merchants in 2022, the fraudsters tested the scheme on smaller merchants throughout 2023. Their success prompts concern that triangulation fraud will be even more frequent this year.

It is difficult to calculate the loss impact of this complex crime; however, one estimate totaled merchants' November 2022 loss at $660 million. Considering that the fraudsters struck at the end of the month, near the end of the year – and that financial institution impact is not included in the estimate – the actual financial loss could easily be a billion dollars or more. The crime also costs time, revenue, and merchandise and, as fraudsters often exploit victims of human trafficking as "store employees," it exacts an enormous human toll.

The criminal ring is resourceful, using multiple methods to clear process hurdles. Fraudsters may manipulate addresses, use re-shippers to cover their tracks, or even launch a Distributed Denial-of-Service (DDoS) attack against merchants' primary address validation services - during the Black Friday 2022 sales, that approach forced merchants to use less effective validation techniques. There is proof of similar attacks taking place again in 2023 and likely tied to the same criminal ring. They are employing machine learning techniques and targeting even more third-party fraud service providers. When standard fraud detection services are unavailable, this forces merchants to use alternative validation, as nobody is willing to stop sales on such a critical day.

Criminals schedule the scheme for the holiday season because merchants are less alert to suspicious delivery behavior – It is not uncommon for gift purchases to have different billing and shipping addresses. Moreover, the logistics of online marketplaces are complicated, so shoppers are accustomed to receiving purchases labeled under a

business name that differs from the original merchant's. As such, there are limited signs that the shopper did not experience a legitimate purchase.

Indeed, the complexity of the scam makes it difficult for any party to realize that the fraud is connected to a larger scheme. This perpetuates the crime and limits visibility on the scope of the damage to the victims.

It Has a Big Impact

When the fraud is eventually discovered, consumers are left with charges they didn't make, merchants are exposed to chargebacks and reputational damage, and financial institutions are faced with managing disputes and reissuing cards. Worse, some of these schemes use victims of human trafficking to staff fake retail sites. Every corner of the triangle is harmed.

Victim Role	Impact
Issuing financial institutions / processors	• Dispute time and expense • Card replacement time and expense • Cardholder trust • Noninterest income if card use not resumed • Potential financial loss if there is no merchant recourse
Legitimate merchants	• Chargeback time and expense • Potential loss of original purchase revenue and merchandise • Shipping and handling expense • Brand reputation
Online shoppers	• Likely loss of trust • Fraudulent charges until refunded • Time • Inconvenience
Staff of fake merchant / scam victims trained to commit fraud	• Loss of freedom and all connections • Potential criminal charges
Other impacted parties	• Address validation firms – DDoS attacks • Online platforms' damage to brand reputation

Holiday Shopping Threats

Triangulation Fraud

Steps to Take Now

Building awareness is the first critical step – and it's a necessary one for all of us. Sharing this document in your organization and with peers is important. Using it as a resource to detect and prevent triangulation fraud is vital as well. Perhaps even more crucial is sharing your experiences and insights. You can join FS-ISAC's Triangulation Fraud Working Group and build on the knowledge base that combats the criminal ring behind triangulation fraud. The tables below include summaries of the Working Group's findings to date, including the Indicators of Fraud and Prevention Solutions. The latter includes both reactive and proactive efforts, which will reduce victims' exposure to triangulation fraud.

Indicators of Fraud

- ☐ High-risk card trends – payment velocity
- ☐ Card disputes – unauthorized purchase or merchandise not received
- ☐ Disputed transactions with common dollar amounts or points of purchase
- ☐ New merchant IDs with high volume
- ☐ Multiple unique cards used in short time frames at a merchant
- ☐ High volume of fraud and dispute reports on new merchants
- ☐ Transaction activity on known bad merchant sites
- ☐ Repetitious activity – merchant, amount, timing
- ☐ Billing and shipping address mismatch
- ☐ Merchant site Whois/IP Search Review – new sites, physical address indicators

Prevention Solutions

- ☐ Cardholder education
- ☐ Card fraud detection
- ☐ Alerting tools – internal and cardholder-facing
- ☐ Card risk rules – monitor and implement rules
- ☐ Active compromised card mitigation
- ☐ Dark web monitoring
- ☐ Effective dispute processing
- ☐ Card data analysis and trending
- ☐ Dispute trend analysis and action
- ☐ Card brand engagement
- ☐ Negative fraud/card/site reporting
- ☐ Cross-aggregation of data
- ☐ Billing/shipping address variance controls

Preventing Fraud Takes Everyone

Each corner of the triangle has a role to play in disrupting this scam. Consumers need to make sure they're buying from real stores. Merchants have to double-down on verifying purchases. Financial institutions need to monitor and flag suspicious transactions.

But to get and stay ahead of the criminal group, collaborating and sharing insights is vital, especially given the complexity of the scheme. A little extra vigilance can help ensure a positive holiday shopping experience for everyone.