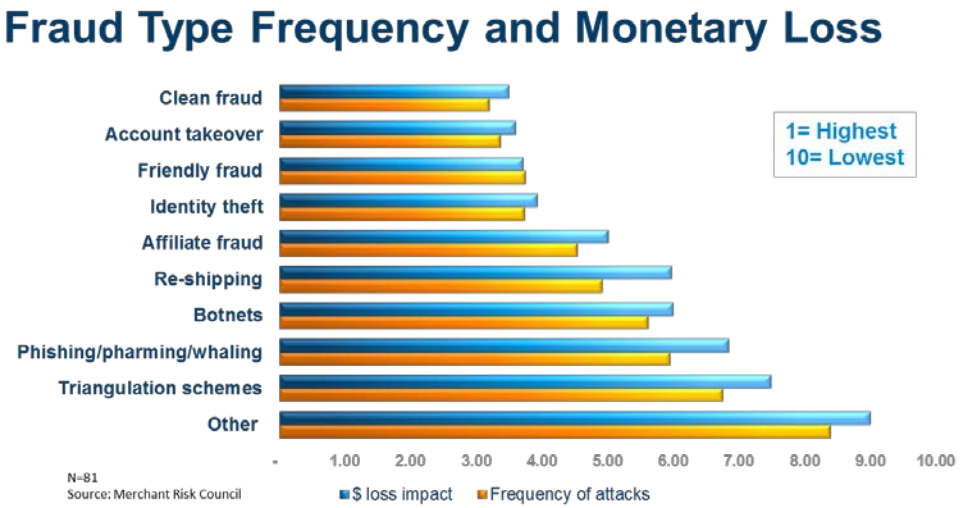
CyberSource®
the power of payment

Questions and Answers from the Top 9 Fraud Attacks Webinar

Q1: Can you show the slide which had the list of all types of fraud ranked by frequency, once again?



Q2: As a web vendor, what kind of information should I have in order to fight chargebacks on physical goods? Order numbers, shipping numbers, IP addresses, etc.? What about intangible goods?

The type of information needed will vary depending on the chargeback reason codes and type of merchants, but the basic information needed to fight every chargeback include:

1. Address verification match to the billing address.
2. Billing address and ship to address verified. Preferably they should be the same.
3. Positive CVV code.
4. Tracking information showing goods were shipped to a verified address and signed for (if possible).

Since there's no proof of delivery for digital services, intangible goods etc., you may want to also show IP address or email communication to support your case.

Q3: Are there any specific fraud issues related to mobile wallets?

The nature of the mobile wallet, with access to multiple payment methods, may be vulnerable to account takeovers. However, mobile wallet is an emerging payment channel. In a recent survey by the Direct Response Forum (DRF), a majority of the retailers reported mobile transactions to be less than 2% of their sales and over half reported having limited visibility into the mobile channel. So it's important to monitor mobile transactions to determine if the risk level begins to rise.

Q4: What tools are available to help identify abandoned and/or foreclosed properties?

You can search Federal, State, and County assessor records as well as real estate search engines such as Zillow and Trulia. Multiple paid third-party tools are available as well.

Q5: Do you feel a larger manual review team will effectively combat these fraud attacks? Or just having the proper technologies in place?

Having a review team is your first line of defense in noticing new fraud trends, but it is more effective when used in conjunction with an automated screening system that does have the proper technologies in place. That way, you can maximize the number of orders screened while keeping your fraud rates low. It is also important to fine tune your system so that you review only those orders with suspicious elements, based on your business rules or prior suspect markings. The key is optimizing your operational metrics so that you continue to keep your fraud costs low while improving your efficiencies and customer experience.

Q6: Any advice for friendly fraud with digital transactions?

Digital merchants should consider having a proactive verification process in place, such as verifying the email, phone, or bank information. This is especially important for organizations that cater to a younger audience (minors). In addition, to prevent further friendly fraud attempts, consider a proactive tracking process, for offenders, typically through a negative or blacklisting process.

Q7: Do you have a list of common locations that initiate triangulation fraud, for instance Nigeria, Jamaica, etc..?

Locations vary by industry, but the most prevalent regions include Western Africa, Eastern Europe, and Southeast Asia. Typically, the fraudster would have resources in those regions.

Q8: How do we differentiate between proxies and VPNS?

The device fingerprinting technology embedded within Decision Manager captures additional TCIP/IP packet header attributes, which enables the analysis of the network connection type from an originating device, including Ethernet, 3G, WiFi, VPN and others.

Q9: I would like to know how you determine the browser language - this would be very useful for the business I am working for based on the kinds of fraud we're seeing.

Browser language is a characteristic identified by the Decision Manager device fingerprint feature.

Q10: Can you expand on how to protect ourselves against affiliate fraud?

If you have an affiliate-based business model, consider installing an affiliate verification process and analyze their performance on a monthly basis (at minimum). If your business does not use affiliates, then consider using a brand protection service for potential false listings by others selling your products through their sites.

CyberSource®
the power of payment

Q11: With buy-online-and-pickup-in-store now available by more merchants, what type of fraud is being seen? What can be done to reduce/prevent?

Many fraudsters use the in-store pickup in conjunction with shipped orders as a way to bypass fraud screens, because merchants tend to consider orders with in-store pickup as less risky since they can check customer information at the store. While fraudsters have no intention of picking up the product in the store, the merchant is more likely to ship the other part of the order if an in-store pickup is associated with it.

Q12: What are the key features we need to keep in mind when implementing mobile device finger print?

Key features to look for in a mobile device fingerprint include the ability to detect true IP, proxy piercing, and fuzzy matching. Fuzzy matching is a technology used to identify when fraudsters rotate features of the device to make it look like a different machine by changing browsers, language, etc. In addition, mobile device data is only one source of data to detect fraud; it should be correlated with other payment details, to provide a better assessment of risk.

From there, you would essentially apply the same practices as you would for any other transaction. Start from the assumption that a mobile order, regardless of whether it comes from a custom app or not, should be treated just like any order, and then build your rules from there.

Q13: How do you get a "real" device fingerprint for a computer that is part of a larger botnet network?

Decision Manager uses proxy piercing and fuzzy matching device fingerprint technology to determine the true IP of the device that the fraudster is using to route transactions through the botnet computer.

About CyberSource

CyberSource, a wholly-owned subsidiary of Visa Inc., is a payment management company. Over 370,000 businesses worldwide use CyberSource and Authorize.Net brand solutions to process online payments, streamline fraud management, and simplify payment security. The company is headquartered in San Francisco and maintains offices throughout the world, with regional headquarters in Singapore (Asia Pacific); Tokyo (Japan), Miami/Sao Paulo (Latin America and the Caribbean), and Reading, U.K. (Europe/Middle East/Africa). CyberSource operates in Europe under agreement with Visa Europe. For more information, please visit www.cybersource.com or call 1-888-330-2300.