Frauds prevailing in E-commerce and Measures of Prevention

Online fraud has grown at startling pace over the last few years, and e-commerce companies need to be highly aware of the many sophisticated tactics criminals use to target them. This article basically covers the three key areas,

1. Types of E-commerce fraud
2. Signs to spot the potential illegal activity
3. Prevention of E-commerce fraud.

"Online fraud" can be defined as illegal activity wrought by a cyber-criminal on a website. It results in unauthorized or otherwise fraudulent transactions, stolen merchandise, and/or wrongful requests for a refund.

Types of Fraud:

1. Identity Theft:

Identity theft results in a cyber-criminal stealing another person's sensitive data and using it to conduct transactions on ecommerce sites as the victim. These transactions are typically paid for by the retailer, as the credit card companies will initiate chargebacks on behalf of the victim. This leaves a retailer without the original merchandise and without the money to cover the loss. It is highly unusual to recover the stolen merchandise or prosecute the criminal.

2. Chargeback fraud:

A customer orders items from the website using a payment method that can easily be pulled (think credit or debit card). Once the items are safely shipped or otherwise out of the retailer's control, the customer initiates a chargeback, stating that their identity was stolen. They then keep the merchandise for free. Many times, the customer is using their own, legitimate credit card.

3. Friendly fraud

Friendly fraud is nearly identical to chargeback fraud, except that it is done without malicious intent. In the case of friendly fraud, the transaction was placed by a true customer, and the chargeback is initiated for something innocent like believing their package to be stolen or not recognizing the merchant's name on their credit card statement. Subscription retailers face this type of fraud often with customers who didn't understand there would be recurring charges.

4. Clean fraud

A cyber-criminal perpetrating clean fraud uses a stolen credit card in such a way that they are able to avoid alerting the fraud detectors. Often this is because the criminal has stolen enough information about the credit card holder that they can easily pass the transaction off as legitimate. As an e-commerce vendor, this type of fraud can be hard to spot because the data is so clean, hence the name.

5. Affiliate fraud

Affiliate fraud is one of a number of fraudulent activities that do not focus on a payment method. Affiliate fraud means that a cyber-criminal manipulates the data collected by the affiliate link given to them by a retailer to make the retailer pay them far more than they are owed. This can be done through an automated process or it can be accomplished by real people using fake profiles. Frequently, the criminal uses a variety of methods in order to avoid setting off any red flags.

6. Merchant identity fraud

Merchant identity fraud is rather simple: the cyber-criminal sets up an online store and entices a victim to purchase something, which they typically list for an impossibly low price. Then they disappear and never ship the item.

7. Advanced fee and wire transfer scams

This is the classic "Nigerian Prince" scam. The cyber-criminal asks for money upfront, in return for a lot more money later. While the Nigerian Prince scam is formulated to specifically target individuals, scammers have come up with a practice that targets businesses, specifically ones that provide services. They'll ask you to send the third-party business some money, which they assure you will be paid back and far more.

Signs to spot the Potential Illegal Activity:

1. Inconsistent order data

A basic and major red flag for fraud is inconsistent data within an order. This contradictory information could be that the zip code and city don't match up, or that the IP and email addresses don't line up. While a real customer can certainly make typos, it's far more likely that a cyber-criminal will make a mistake by guessing wrong information.

2. First-time customers

As exciting as it is to get a new customer, scammers typically appear as first-time customers. They don't often return to victimize the same company more than once, so as to avoid generating suspicion. While being a first-time shopper alone should not necessarily attract your attention, you may want to ensure that your security features carefully monitor your first-time buyers.

3. Customers who make multiple orders from different credit cards

Most consumers have no more than three credit cards, so you should be suspicious of shoppers who use more than three cards when shopping on your site — especially if they try to use those cards one after another. If a customer puts in multiple orders on many different credit cards, whether in one sitting or over a long period of time, you could be dealing with a cyber-criminal.

Variations on this sign include:

- Multiple transactions under the same billing address going to different shipping addresses.

- Multiple transactions under the same billing address going to different shipping addresses.
- Multiple credit cards used on the same IP address, even if they are not billed or sent to the same person.
- Multiple transactions on the same card in a short period.

4. Unexpectedly large orders (especially those that contain duplicates of products)

Scammers are known to drop significant amounts of money when they make fraudulent purchases – usually, far more than any of your typical customers would spend. A large order may be exciting at first, but you'll certainly want to look into it. If they have paid for expedited shipping on that large order, that's even more of a red flag. It indicates that the scammer is interested in getting their hands on the goods before they get caught.

5. Any data that's clearly fake

This probably sounds obvious, but you want to watch out for any data that seems made up. It's not that difficult to catch fake email addresses (has no@yahoo.com ever been a real address?), and fake phone numbers can even be found by sight alone. For instance, any number with the area code "555" is a fake.

6. Multiple declined transactions to the same customer

Again, while people do make typos during a transaction, one person attempting to use the same card while inputting the numbers wrong several times can indicate someone who's trying to guess at a few of the numbers.

How to prevent E-commerce fraud:

1. Implement fraud prevention policies
2. Never stop monitoring
3. Have a secure web shopping experience using HTTPS
4. Don't share the passwords, CVV with anyone and frequently change the passwords.
5. Work with a reliable third-party payment processor
6. Do not store customer data unless necessary
7. Comply respective laws applicable
8. Keep your software up-to-date
9. Use protection services
10. Train your staff to protect their own data
11. Endpoint authentication
12. Biometric security features

Contributions made by: Srikar Gupta
Sources: https://www.clearhaus.com/blog/fraud-in-ecommerce/