If you are running an ecommerce store, you need to protect your business and your customers against potential threats – a process which is often overlooked among other business processes like quality control, product sourcing, marketing and customer services. While E-commerce fraud is not something new, it has been constantly on the rise since the past decade, and online stores need to be more well-informed than ever about different schemes used by cybercriminals for online fraud.

Fraud is not exclusive to credit cards, whether they are [magnetic strip embedded](cardzgroup.com) cards or smart cards. Rather, alternative payment methods are also attracting criminals. They have become more sophisticated with the use of malware to steal bank account details and use them to log in via computers, phones and tablets. These threats need to be taken seriously to reduce and combat the impact of fraud on your ecommerce store.

Let’s look at five of the most common types of ecommerce fraud schemes to help you leverage from and prevent the next fraud attack on your online store.

1. **Friendly Fraud**

Also known as chargeback fraud, this method works by buying a good or service online in a normal manner, and then deliberately requesting a chargeback from the payment processor by claiming that their account was hacked or credit card details were stolen. The bank or credit card company reimburses the amount – which still must be paid by the retailer, but the customer gets to keep the item.

Friendly fraud method is more common with services such as those in gambling or adult industry. It also tends to be combined with re-shipping, where a customer makes a purchase using stolen data and instead of receiving items at their home address, uses a middleman’s address details, who then forwards the goods after receiving them.

In other instances, a criminal may buy an item from your store and claim that it didn’t get delivered, while telling their payment processor that they returned the item but never got a refund – or that they cancelled the order but the item was still delivered to them.

Whatever the scenario, using a chargeback management software can help you deal with disputes and reduce the likelihood of loss occurring as a result of friendly fraud.

1. **Triangulation Fraud**

The name, triangulation fraud, comes from the fact that it involves three parties – the legitimate shopper, the fraudster and the e-commerce store.

The first party, the fraudster, creates an online storefront on an ecommerce site like Amazon or eBay and offers very low prices for goods in high demand to the second party, the legitimate customer. In many cases, they add an additional bait. For instance, they mention that for immediate shipping of goods the customer must purchase via credit card. This way, the store collects credit card and address information of many customers.

The fraudster then not only collects payment from the customer on its fake store, but also uses their stolen information to purchase goods from the third party, the legitimate e-commerce store and ships them to the customer.

1. **Interception Fraud**

In this type of fraud, a cybercriminal places an order on an ecommerce store where the shipping and billing address match the information linked to a stolen card. After placing the order, they aim to intercept the package and take the goods for themselves in one of the following ways.

* Ask a customer service representative to change the shipping address before shipment.
* Contact the shipper or courier to reroute the package to a different address.
* If they live in proximity to the actual cardholder’s address, they may wait for the delivery to arrive and receive the package as their own.

1. **Card Testing**

This is a widespread tactic that is used to defraud ecommerce stores. In 2017 alone, card testing fraud accounted to 7 percent of bigger ecommerce merchants and 16 percent of entire ecommerce fraud.

In a card testing fraud, a fraudster tests the validity of a stolen card with the intention to use correct card credentials at a website. They visit ecommerce websites and make small test purchases, usually with bots or scripts to test multiple card numbers in rapid succession. They target websites that show a different response for each decline. For instance, if a card is declined because of incorrect expiry date, they get a different response – and know that all other information is valid except the expiry. They then just need to find the correct expiration date for the card to work. The initial purchases are very small, since the main purpose of the fraudster is to see if the card can be used to complete a transaction. Once they know that the card works, they start making bigger purchases.

1. **Identity Theft**

In identity theft, a cybercriminal adopts the identity of another person, creates credit cards in their name and carries out transactions from the victim’s identity.

To do this, rather than creating completely new fake identities, they target personal information of real people, such as names, email and home addresses, as well as financial information. They then shop online under a someone else’s identity and pay with their credit card information or bank account.

Identity theft is rapidly increasing with the increase in scope and number of data breaches. It is also very difficult to identify because the cybercriminals behind identity theft are often sophisticated hackers.

**Defending Yourself Against Fraud**

There is no denying that the world of online fraud is complex. With time, fraudsters are now more knowledgeable and intelligent and often accomplish their goals with out of the box techniques. Whether your business is small or big, using a high-quality software solution can make a big difference. Moreover, if you are vigilant and informed about prevention methods, you can considerably mitigate risks associated with ecommerce fraud.