If you are the owner of an Ecommerce store, you must be wary of potential threats that damage your business and customers. Businesses are often so immersed in other processes like product sourcing, quality control and customer services – that they tend to overlook their security. Though E-commerce fraud is not a new thing, it’s consistently on the rise. For this reason, online businesses need to stay vigilant and educate themselves about different schemes cyber criminals use for conducting online fraud. It is also advised for businesses to take help from a cyber security consultancy to manage their security policies and procedures.

**Let’s have a look at five most common types of E-commerce fraud schemes.**

1. **Friendly Fraud**

Friendly fraud is also known as chargeback fraud. In this type of fraud, the criminal buys a good or service online, and then purposely requests a chargeback from their payment processor. They make this claim on grounds that their credit card detail was stolen or account was hacked. The payment processor such as bank or credit card company pays the amount back to the customer, which still has to be paid by the retailer – and the customer also gets to keep their item.

1. **Triangulation Fraud**

The name triangulation fraud refers to the involvement of three parties – the fraudster, legitimate shopper and the Ecommerce store.

The fraudster first makes an online store on any e-commerce site like eBay or Amazon, and offers affordable price for high demand goods to the legitimate customer. They then collect payment card information of various customers and use it to buy goods from the third party – the real e-commerce store, and delivers them to the customer.

1. **Interception Fraud**

In an interception fraud, a cyber-criminal buys from an Ecommerce store providing shipping and billing address of a stolen card. Once the order is placed, they intend to “intercept” their package and get those good in some of the ways:

* Call and ask a customer services officer to change their shipping address to a different location before shipment
* Contact the courier to deliver their parcel to a different location

1. **Card Testing**

This is another type of Ecommerce fraud scheme where the cyber criminal tests a stolen card’s validity with the intention of using real card credentials at website. They make small purchases from E-commerce websites usually with scripts or bots to test numerous card numbers in quick succession. They then target those websites that get different responses. For instance, if a card is declined because of incorrect date of birth, the hacker just needs to find the correct date of birth to enter the system then.

1. **Identity Theft**

In an identity theft, a hacker impersonates as another person by using their identity such as name, phone number, email addresses and credit card information. They then use this identity to shop online using the other person’s bank account or credit card information.

**Defend Yourself Against Fraud**

To protect against these types of frauds, always use a high-quality software and stay vigilant. Always keep yourself informed about what type of Ecommerce fraud schemes exist and how to avoid them. You can also get services from a cyber security consultancy firm to carry out risk assessment of threats your business may face against ecommerce fraud.