Credit cards in the wrong hands can wreak havoc for the owners. Unfortunately, with the increase in the use of digital technology, credit card scams are becoming more and more common. Scammers and cybercriminals are finding more ways to commit this kind of fraud. Although, credit card fraud can happen with anyone who is using it,there are multiple ways for you to prevent yourself from being a victim. Let's dig deeper into what this fraud is before we can move on to ways to prevent it from happening.

## **What is Online Card Fraud?**

Online card fraud refers to the misuse of credit or debit cards by taking over the owner's details. Due to the increasing trend in online shopping, scammers and cybercriminals have access to user details which they can use to their advantage. A lot of scammers don't even need the card physically to commit the fraud. Moreover, they don't even need you to physically swipe one.. As scary as it sounds every bit of it is true and is the reason why credit card theft is becoming so common.

## **Preventing Different Types of Credit Frauds**

Let’s look at some common types of credit card scams, ways you can prevent them, and what to do if you have been scammed already.

**Card-not-present (CNP)**

One of the most common types of fraud is done through card-not-present transactions. As the name suggests, the scammer does not need the card physically to commit this type of fraud. All they need are the details of the victim, which they can acquire when someone is making an **online transaction.** The growth of the eCommerce industry is a major contributor to the growing cases of this type of fraud.

CNP fraud is a big threat to both buyers and sellers. It is advised to merchants to watch out for this fraud by monitoring any unusual activity on the site. They can also develop a more proactive approach by adding an extra layer of authentication. This way scammers will have to undergo another security layer which might discourage them from committing fraud. On the other hand, buyers should be skeptical about entering their card details and should only choose legit platforms for online shopping.

**Skimming**

Skimming frauds occur when a credit card device or an ATM is programmed to copy the details of the credit card onto a magnetic strip and later uses it to counterfeit the credit card. Alarmingly, skimming can also take place if a person walks past you with a credit card skimming machine. This type of fraud requires the user's PIN.

An ATM that is tampered with will most likely have a micro-camera installed within which will note down the PIN code. Similarly, if the activity is done through a credit card machine at a terminal, the person-in-charge will try to read off the PIN code being entered.

To prevent such fraud from taking place, one should always hide the keypad when entering his/her PIN code. If you are in a public place you should keep your card in the inside pockets of your wallet. Moreover, if you get the feeling that an ATM is tampered, you should report it to the local authorities immediately.

**Lost and stolen card**

As the title suggests, this type of fraud will occur only on those cards which have either been lost or stolen. If you have suddenly lost your card or have misplaced it then don’t wait for the worst to happen – immediately contact your credit card company and get your card blocked.. If your card lands in the wrong hands it could have disastrous consequences.

Luckily, a lot of banks have the option embedded in the bank’s mobile application to immediately block the card in case it is lost or stolen. This has made it convenient for users to take action. Moreover, if you have decided to stop using a credit card don’t just throw it into the waste bin. You need to cut it into small pieces so that no piece of information on the card can be leaked to criminals.

**Application fraud**

Application fraud is one of the oldest kinds of frauds that scammers have been committing over the years. The person who is committing this fraud assumes another person's identity and receives their credit cards. They even use a temporary mailing address to receive these cards on their doorstep. However, banks have now raised their security bars high and they have regular monitors to confirm the addresses of their customers. The processes at banks have become more and more thorough to ensure that the account accessories reach the right person.

## **Key Takeaways**

The best way to protect yourself from a scam is to be vigilant when it comes to online transactions and keep your credit card in a safe place. If you suspect any suspicious activity don't think twice and inform your credit card company. An online credit card fraud can take place anywhere and anytime but with the right steps, you can mitigate the impact.