Mobile and contactless payments have seen a rapid increase in popularity, particularly in the post COVID times. However, its increased usage has also given rise to contactless payment scams, since removing the need to use a PIN code has offered more opportunities to criminals.

Let’s have a look at how we can make contactless payments more secure and avoid becoming a victim to contactless payment fraud.

1. **Keep Your Contactless Card in a Secure Place**

This is very important when using public transport, since some scammers carry card readers in these places. These card readers are easily available and allow a scammer to carry out a [transaction](http://www.cardzgroup.com/ContactLessSmartCard.html) by being in close proximity to a card holder. To avoid raising an alarm, they type a value that is less than the usual limits (such as $25 to $50), and hold the device close to people’s pockets or wallets. Even without a specialized device, you can also install card reading applications on your smartphones

To avoid this, it is important to never keep contactless cards or wallets in your back pockets. Try to keep them somewhere secure and covered, such as a front pocket or a hand bag to avoid close proximity of a scammer with your contactless payment card.

1. **Invest in a Wallet that Blocks RFID**

Even if you keep your wallet securely tucked inside your pockets, there is still a chance that someone skims close enough to scan your card. To avoid this from happening, you can buy specialized wallets to safeguard your contactless cards. These are called RFID-blocking wallets, which look like a metal case with different folders inside. These wallets help block radio waves between the RFID chip in your card and the card reader.

1. **Create a Strong PIN for Contactless Mobile Payments**

Many digital wallets such as Apple Pay authenticate a payment using fingerprints, but if your smartphone verifies payment details with a PIN or pattern, using PIN is a more secure option. For payment authentication, you may want to keep the same PIN you use for unlocking your phone, but this is similar to using same password for different accounts. This is not advisable and it is always safe to keep a separate PIN for your wallet.

Similarly, when choosing a PIN, never use any number from your Personally Identifiable Information (PII), as it can be easily guessed by a criminal, such as your date, month, or year of birth.

1. **Never Let Your Card Out of Sight**

When making payments for a product or service, never hand over your card to someone to carry out the transaction for you. Instead, try to do it yourself. Most of the times in restaurants, we tend to hand over our card to the staff to pay our bill by taking it to the card reader, which is mostly at another end of the restaurant. Either go and pay the bill yourself or ask the staff to bring over the card reading machine to your table, but never let your card out of your sight.

1. **Keep a Check of Your Transactions**

It’s always a good practice to check your monthly bank statement thoroughly, to spot any payment scams or credit card fraud. If you see something that you cannot recognize, immediately contact your credit card provider or bank. In most cases, if you were scammed, your amount will be refunded. You will also need to cancel your existing card and request for a new one.

However, there is still a security drawback to cancelled credit cards, which is offline payments. Although most retailers now use online systems to check card credentials on the go, many of them still use offline payment processing. This means that their card reader creates a list and processes payments at a later time. Online payments help to immediately verify the authenticity of the card. However, offline takes time to check if a card is still authorized or cancelled, and allows scammers to make transactions with cards that were already cancelled. Hence, it is important to check your bank statements and claim for refunds if any unknown payment was done with your cancelled card.

**Detecting and Investigating Contactless Card Payment Fraud**

A contactless card fraud investigation is usually a collaborative process to consider facts and decide whether the blame is on merchant or the cardholder. Typically, it’s the banks that carry out the investigation, and not the credit card companies. Although these companies set the rules to follow in case of fraud, most payment disputes are handled by the issuing bank of the cardholder.

The investigation process often involves the customer making a complaint. The bank reviews and examines the transaction to decide whether the customer is making a reasonable claim or not. Based on the evidence, banks decides to either reject the complaint or file a chargeback on behalf of the customer.

**Evidence Used in to Conduct Investigation**

Different pieces of evidence can be used to conduct contactless payment fraud. This can include:

* **Geolocation Data:** The place from where the card was used, and if it matched with cardholder’s location or not.
* **IP Address:** The buyer’s IP address in case of an online transaction, and if it matched with that of the cardholder.
* **Behavioral Pattern:** Is the purchase seemingly unusual given the typical buying pattern of the customer? Have they purchased similar items before?
* **Account Activity:** Was this a one-time incident or were there back and forth transactions from the cardholder’s account?

**Conclusion**

Even with all these and other security practices in place, you could still become a victim of contactless card fraud. However, it is important to follow best security practices, stay vigilant, and make the most of the convenience that comes while making contactless payments.