**What You Need to Know About RFID Payment Cards**

**Introduction**

With new innovations in credit card technology, it is becoming easier to make payments, while increasing transaction security at the same time. One such development in payment card industry is the use of Radio Frequency Identification, or RFID technology. With the help of this technology, users are able to make payments by putting their cards close to the card reader, hence, called “contactless smart cards”.

**What are Contactless RFID Smart Cards?**

Contactless smart cards use the EMV protocol to communicate with devices enabled with Near Field Communication (NFC). Every card has an antenna embedded inside it which enables it to communicate with the reader without physical contact.

RFID cards can find their applications in access control, public transport payments, parking, cashless vending, toll payment, and more.

**How do they work?**

RFID has been here since a long time now. It is a term that describes technology based on radio frequencies for things such as scanning items at grocery shop or getting office access through a key fob.

The RFID chip in the contactless card is not powered. It gets power transferred to it in the form of Radio Frequency when the card comes in vicinity with the contactless payment terminal. Since there is no PIN code or signature required for contactless purchases, banks usually put a limit to maximum purchase per transaction, such as $50.

The Near Field Communication (NFC) technology also makes it impossible for a fraudster to link the card with its original [identity credentials](cardzgroup.com) by using tokenization. This is made possible by replacing the card’s actual number with another unique set of characters and numbers for every transaction that is carried out. This token is only valid for one transaction; hence, the same information cannot be used twice.

**Advantages and Disadvantages**

Contactless RFID cards are faster and secure and have the same protection like other smart cards. When connected to a smart phone, they can show features such as remote deactivation, virtual card provisioning, payment history and user-configured PIN. The tap-to-pay method of an RFID card allows for convenient transactions, making it particularly useful at transit venues.

Many smartphones today come with NFC capability and can use applications for reading data stored in contactless cards. There are also open source software programs available for reading and extracting contactless card data, which can then be used for building NFC application. This ease of use and availability can go against the cardholder. An attacker can use an NFC enabled phone coupled with an app or an RFID reader to extract data from potential victims in a crowded public space and steal their card data – an act known as “electronic pickpocketing”.

**Why We Don’t need to Worry about RFID Shielding?**

As a solution to electronic pickpocketing, many companies have developed their solutions of RFID shielding products, which they claim can protect a user’s information from being stolen. Companies like Identity Stronghold [1] have a wide range of RFID blocking products including wallets, shielded sleeves and bags. RFID blocking surely does stop unwanted transmission, but there is very little evidence of real-life practical RFID based thefts. It is, therefore, not as big a threat as it seems and not something too big to worry about.

According to Eva Velasquez, CEO & President of the [Identity Theft Resource Center](http://www.idtheftcenter.org/), there is little evidence which supports the likelihood of RFID based theft. “Thieves have better (and quicker) ways to obtain this info. “For one, it’s cheaper for a criminal to buy credit card numbers on the Dark Web instead of purchasing a RFID scanner. They could also do some hacking and steal these numbers much faster than going person to person with a scanner.”[2]

Roger Grimes, a computer security veteran says, "There's probably hundreds of millions of financial crimes being done every year and so far, zero, real life RFID crime. An RFID hacker has to make sure that there's a lot of people walking by with RFID-enabled credit cards, [and] there's good chance they'll be caught on closed circuit cameras nearby, versus, I can for a lot less risk, go online on the Internet and buy thousands" of credit cards, their information and security codes "for literally a couple of a bucks a piece."[3]

**What Happens if your Card is Stolen?**

Contactless RFID cards come with a transaction limit, so it’s not like a card thief can buy a holiday ticket or a new car with your cash. Some providers also have maximum limits per day on cards, which restricts the damage that can be done with contactless payments.

Also, it is very likely that your stolen card is used for online purchase, since transaction limits are usually not the same online. But whether a card is contactless or not, the impact on online transactions is the same.

**Are Contactless RFID Payment Cards the Future?**

As more merchants are getting onboard and more consumers are embracing digital payments, RFID contactless cards are going to stick around.

**References**

1. <https://www.idstronghold.com/>
2. <https://lifehacker.com/why-you-don-t-need-to-worry-about-rfid-shielding-1818626171>
3. <https://www.npr.org/sections/alltechconsidered/2017/07/04/535518514/there-are-plenty-of-rfid-blocking-products-but-do-you-need-them>