CARDING - CREDIT CARD THEFT AND FRAUD

Shibu Shashank*

ABSTRACT

As we all know, we are living in a 'Digital Era,' in which our Indian economy is attempting to become a Cashless Economy, in which everyone has access to a Digital Payment System using plastic money, like Credit and Debit Cards provided by the bank. Because it is a type of transaction in which money is made straight from one bank account to another within seconds. However, when the transaction occurs, the database saves the details of the card used in the transaction. It carries the details of the card. The key objective of this article is to make the reader aware of how to be secure and protect themselves from being a victim of such kind of fraud so that our money, bank account, and personal information remain protected. The explanations and preventative measures provided in this paper are more likely to assist those groups of people who do not have much information about these types of dangers and new technology, allowing them to be wary of these types of thefts that occur on a wide scale even in India.

Keywords: Carding, Fraud, Digital Era, Cyber-crimes, Cyber Laws

* B.A.LL.B. (3rd Year) Symbiosis Law School, Nagpur, Symbiosis International (Deemed University).

CARDING - CREDIT CARD THEFT AND FRAUD

Introduction:

According to James Chen, *"Carding is a form of credit card fraud in which a stolen credit card is used to charge prepaid cards. Carding typically involves the holder of the stolen card purchasing store-branded gift cards, which can then be sold to others or used to purchase other goods that can be sold for cash. Credit card thieves who are involved in this type of fraud are called carders[1]."*

The term 'Carding' is generally defined as stealing someone else's Credit Card details on the web and further using it for purchase of goods or services available on the Internet, without the knowledge of the owner of the card. It was originally started in Toronto, Ontario (CANADA) and then it gradually spread to other countries as well including INDIA. The purchase of Credit Cards take place on the DARK WEB and not on the regular internet servers that we use on daily basis. Money theft is not the only issue via unofficial use of credit cards, but also the breach of personal information of the user that can be accessed by the hacker who is involved in the process. Hence Cyber security come into picture, which is indeed one of the most important field of LAW that actually deals with all kinds of Cyber threats including carding as well.

Carding has evolved significantly in the last several years. The activities surrounding theft and fraudulent use of debit and credit cards including Computer Hacking, Phishing, and other means of threat. Persons who engage in the activity of Carding are referred to as 'Carders'. We can often find these Carders on internet. They are mostly active on Social Networking Websites like Instagram, Facebook and others. They claim that they are genuine seller of those products which they are dealing with, but certainly they are not. Isn't it illogical to say how can someone sell a product that cost Rs.1,00,000 in the market to such a price point as low as Rs.10,000? Absolutely they are fake sellers, or simply they are Carders.

First, they purchase credit cards of real users from the Dark Web which cannot be accessed by any unprofessional or a regular internet user who don't have much knowledge about this. Then

[1] https://www.investopedia.com/terms/c/carding.asp

they use those cards to purchase products for the same price as displayed from any E-Commerce website. They use different address to receive those products so that they don't get caught. Later they compile all the products and they start advertising those products which are available to them for selling. People unaware of these carded products, just go ahead and buy the product that they want at a very cheaper amount. I mean, obviously! Who don't what products at their 10% of the actual cost of the item. But what happens in majority cases is another twist here.

When the seller agrees to the buyer that he is ready to dispatch the product of the choice of buyer and eventually, the seller demand some amount of money either for dispatch of product or some kind of processing charges from the buyer. As soon as the buyer pay certain amount as was told earlier, the seller all of a sudden disappears! In majority of the cases, the buyer blocks the user after taking the money and the money is actually lost from the side of buyer. There is no chance of tracing as well because they use FAKE Mobile Numbers and Email Addresses. The Credit cards that they use for transaction are actual cards and actually the money gets debited from the card holder's bank account. These are the Black Hat Hackers who already has intention to steal someone's money for their benefit without any moral thinking that they are actually stealing someone's hard earned money.

As we all know, we are living in a 'Digital Era' in which our Indian economy is trying to be a Cashless Economy where everyone can have access to Digital Payment System via plastic money, like Credit and Debit Cards issued by the bank. As it is a form of transaction in which the payment is directly done from one bank account to another within seconds. But as the transaction happens, the database actually stores the details of the card through which the transaction happened. Either Visa, MasterCard or RuPay Card, it holds the details of the card – 16-Digit Number, Name of the holder, Date of expiration and CVV which is a 3- digit number which is the most essential part of a credit card for any transaction to happen on the Internet.

Types of Carding –

1. Carding Online

   The term "carding online" simply refers to the use of stolen credit card information to make online purchases of products and services from internet sellers. Credit card issuers have put a three-digit number that is present on the back end of the card, often called as

CVV, to prevent fraudulent transactions, which internet transaction gateways generally need as part of the whole transaction process. Therefore, a carder will require the CVV to process the transaction. To avoid being detected, carders who buy products online have them delivered to a location other than their own. Carders who engage such process may require the assistance of a "change of billing" specialist. COB services entail gaining online access to the user's credit card account after getting all required account information and changing the billing address to reflect a new shipping address.

2. In-Store Carding

   Another type other than online carding is “In-Store Carding”. In this form a carding, a counterfeit credit card is generated from the payment terminal or the POS Machine by using a Card Skimmer that are often used in ATMs as well in some countries including India. In-Store carding require a carder to physically check into the store, as a result, it is riskier than online carding from the perspective of the carder. A carder will need several pieces of equipment to create a counterfeit card, including laminators, embossers, encoders, scanners, and printers. The carder begins by copying the dimensions of the card onto a white plastic sheet. After that, the carder may use this plastic sheet as the dimensions and the magnetic strip being just same as the original credit card at any vendor or shop that accepts card swipes on POS machines. The carder creates a fake Visa or MasterCard front with the use of a printer. After completing these steps, the carder will have a clone credit card or a counterfeit card that can be used for future transactions.

   As the customers swipe their credit cards on the POS Machine, they are unaware of the fact that their cards are actually being cloned and it can be used anywhere and any transaction made via their clone credit card will amount to their loss as the bank would interpret the clone card as an original one.

It is an offence under the Information Technology Act 2000 (Sec.66C) – Punishment for identity theft

Section 66C provides for punishment for Identity theft as: “*Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may* *extend to three years and shall also be liable to fine with may extend to rupees one lakh."*[2] With the growth in the number of frauds and web crimes, the government is developing improved rules to protect the public's interests and safeguard against online fraud.

*Credit Card Fraud

Innocent users would use and access infected PCs to initiate online payments. Provisions Applicable – Information Technology Act, (Sec. 43, 66, 66C and 66D), Indian Penal Code, (Sec.420)

Real life scenario -

- A 32-year-old man was arrested for credit card fraud as uncovered by Delhi Police[3]. The accused's name was Raju Tevar, and he was detained when Abhay Srivastava submitted a complaint alleging that his ICICI Bank account had been infiltrated and that he had been defrauded of Rs.44,911 using his credit card. In the accused laptop, investigators discovered data from around 30,000 ICICI Credit Card customers. It leads them to believe that the scam might be much greater on a wider scale. After three months of enquiry and investigation he was caught by the police authorities and it was found that one of his friends named Zakir, from whom he stole all the credit card data which he used for further transactions was present and he helped Tevar to breach the personal data of ICICI Customers.
- Delhi police arrested two geeks for credit card theft.[4] Jayshankar Kushwah and Rajesh Rawat, the two accused, bought gold coins from several online purchasing websites using credit cards belonging to unknown persons. They were both Post Graduates in Computer Applications. On April 4, 2016, both of them scammed a businessman identified Gautam, who was cheated for Rs.2.5 lakhs. He lodged a formal complaint in the Police Station after both of the accused used his credit card to make payments on e-commerce websites without his permission and without his knowledge. They were involved in the purchase and sale of carded items, the theft of credit cards, the creation of false government ID

[2] https://indiankanoon.org/doc/118912881/

[3] https://www.dnaindia.com/india/report-mumbai-resident arrested-for-biggest-online-credit-card-fraud-1861136

[4] https://www.indiatoday.in/india/story/delhi-police-busts credit-card-fraud-arrests-2-techies-327331-2016-07-04

cards, and the alteration of fictitious addresses. As a result, they were held accountable and arrested by Delhi Police.

In the year 2017-18, We can observe the amount of cybercrime reports made by users around the country. The shocking reality is that it is steadily rising. Most of the users do not even complain as they think that they will sound foolish in front of the society that they are the victim of carding or credit card theft which comes under cybercrime. Every year, an increasing number of cases are filed in this respect. The difference between the number of lawsuits filed in 2014 and the number of cases filed in 2018 is approximately four times[5]. As a result, it is a big worry when it comes to the security of people's personal information and money. Hackers are targeting social networking sites to promote carded items, and they employ a variety of ways to steal and clone credit and debit cards from consumers both online and offline.

It was observed that during the year 2008 to 2017, number of data breaches and the number of records exposed in Millions, which is indeed a huge amount. And it’s drastically increasing yearly.[6]

Methods of prevention from credit card theft –

1. One must not use his credit card on any third-party E-Commerce website for online transaction without checking the authenticity of the website and the payment gateway as well. Make sure that the payment portal is secured.
2. Never store Credit and Debit Card information anywhere online on the internet. There’s always a chance of risk for the leakage of personal data including credit cards details as well.
3. Avoid International transaction through the Card if possible because those hackers eagerly wait for the transaction to happen via their portal so that they can extract credit card information from that and further sell them to carders for a reasonable price and then those carders use the required details of the user for their benefit.
4. Always check whether the URL on which the payment is to be made has https:// protocol before the complete web address.

[5] Article on Data Breach by Kimberly (US Justice Dept.).

[6] https://www.iii.org/fact-statistic/facts-statistics-identity-theft and-cybercrime

5. Never use someone else's Wi-Fi Network for any transaction via credit or debit card. The user being the admin of the Wi-Fi network can anywhere and anytime extract all the information of the Credit Card.
6. When using ATM Machines to withdraw money from the bank account, always check whether the ATM Skimmer is installed over the card slot or not. These ATM Skimmers can create a clone for the card inserted in the slot.
Make sure to cover the keypad of ATM as well so that if any spy camera is installed to record what then pin you entered can remain hidden from it.
7. While doing any transaction from the card on any Store or Petrol Pump or anywhere where credit card is accepted as a mode of payment via POS Machines, do check if something suspicious or something is attached to the machine as it can record all the details of any card swiped through and hence can create a clone for the same.
8. NEVER SHARE your Credit Card Number, Card Holder's Name, Expiry Date of the Card and the CVV Number to anyone at any cost.
9. Keep a check your Bank Statements regularly so that you can identify any suspicious transaction from your credit or debit card which is not done by you.

What to do if you are Cheated?

In case of any credit card theft or a fraudulent online or offline tra1nsaction, immediately contact your bank and block the credit card as fast as possible. It is also advisable to lodge an FIR at the earliest. Afterall, it's a matter of someone's hard earned money. Be SAFE! Prevention is always better than Cure.!!

It all comes down to the fact that people must be aware of this type of new 'theft' that happen on daily basis and anyone, literally anyone can be a victim of carding in this digital era. Safety measures must be taken in order to prevent credit card theft as most of the methods of prevention were already discussed in the research paper itself. People should be aware while using their credit card for any transaction either online or offline.

As far as carding is concerned in India, it is not even much renowned among the people. Indian Cyber cell is also not much active regarding the same issue, as they don't get much cases from the victims. Some report to the cyber cell, while some don't.

Government is also not that much interested in dealing with this issue nor educating people about the same. Although we can see some campaigns about cyber security and how to protect us from certain threats and that's very good initiative form the Government but that is not implemented on a larger scale actually in our Country. It needs to be done. Safety and privacy should be the top priority. So, in order to distribute information across a big number of Indians, social networks should be leveraged via the internet rather than physical sources.