

ISSN: 2582 - 2942



LEX FORTI

LEGAL JOURNAL

VOL- I ISSUE- VI

AUGUST 2020

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of LexForti Legal Journal. The Editorial Team of LexForti Legal Journal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of LexForti. Though all efforts are made to ensure the accuracy and correctness of the information published, LexForti shall not be responsible for any errors caused due to oversight otherwise.



ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR IN CHIEF

ROHIT PRADHAN

ADVOCATE PRIME DISPUTE

PHONE - +91-8757182705

EMAIL - LEX.FORTII@GMAIL.COM

EDITOR IN CHIEF

MS.SRIDHRUTI CHITRAPU

MEMBER || CHARTED INSTITUTE

OF ARBITRATORS

PHONE - +91-8500832102

EDITOR

NAGESHWAR RAO

PROFESSOR (BANKING LAW) EXP. 8+ YEARS; 11+ YEARS WORK EXP. AT ICFAI; 28+ YEARS WORK EXPERIENCE IN BANKING SECTOR; CONTENT WRITER FOR BUSINESS TIMES AND ECONOMIC TIMES; EDITED 50+ BOOKS ON MANAGEMENT, ECONOMICS AND BANKING;

ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR

DR. RAJANIKANTH M

ASSISTANT PROFESSOR (SYMBIOSIS
INTERNATIONAL UNIVERSITY) - MARKETING
MANAGEMENT

EDITOR

NILIMA PANDA

B.SC LLB., LLM (NLSIU) (SPECIALIZATION
BUSINESS LAW)

EDITOR

DR. PRIYANKA R. MOHOD

LLB., LLM (SPECIALIZATION CONSTITUTIONAL
AND ADMINISTRATIVE LAW)., NET (TWICE) AND
SET (MAH.)

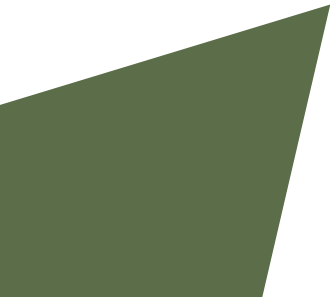
EDITOR

MS.NANDITA REDDY

ADVOCATE PRIME DISPUTE

ABOUT US

LexForti is a free open access peer-reviewed journal, which gives insight upon broad and dynamic legal issues. The very objective of the LexForti is to provide open and free access to knowledge to everyone. LexForti is highly committed to helping law students to get their research articles published and an avenue to the aspiring students, teachers and scholars to make a contribution in the legal sphere. LexForti revolves around the firmament of legal issues; consisting of corporate law, family law, contract law, taxation, alternative dispute resolution, IP Laws, Criminal Laws and various other Civil issues.



Simcard Cloning and Crimes: A Critical Analysis

Gaurav Lalwani

ABSTRACT

SIM card Cloning is criminal behavior that crooks frequently do by changing the Electronic Serial Number (ESN) of SIM by utilizing extraordinary specialized programming. In this action two Sims works at the same time one the bonafide client and another unlawful cloned SIM. The ESN is ordinarily sent to the telecom organization to associate any cell phone/gadget onto the system. By altering Electronic Serial Number (ESN), Preferred Roaming List (PRL), and Mobile Identification Number, with this any misrepresentation an individual can make extortion calls to raise bills from a unique wireless client and perpetrate wrongdoing. It would raise genuine perils to national security frameworks as these SIM cards are being utilized in psychological militant and against national exercises and illicit bank exchanges. The false utilization of specialized gadgets has made the requirement for solid and solid laws for this kind of offense. Rapid increment in innovation Increases the odds of wrongdoing.

Through this paper, the analyst wants to focus on proposals to Increase security by ordering new solid enactment/guidelines and which can cover the parts of the featured theme so the hazy areas in law can be evacuated. The specialist might want to propose a potential arrangement considering this issue and appropriate system of usage of digital security laws to guarantee wellbeing considering expanding casualties of SIM Card cloning in India today.

INTRODUCTION

Cloning alludes to the procedures used to create duplicates of DNA fragments, cells, or organisms. Dolly the lamb was cloned from a six-year-old ewe in 1997, by a group of researchers at the Roslin Institute in Scotland. While the debate on the morals of cloning continues, the human race, just because, is faced with a clearer and harmful variant of cloning, and this time it is your cell phone that is the target. A large number of cell phone clients run in danger of having their telephones cloned. As a cell phone client, if you have been receiving gigantically high bills for calls that you never placed, chances are that your cell phone could be cloned. Unfortunately, there is no chance the endorser can identify cloning. Occasions like call dropping or anomalies in a month to month bills can act as tickers.

Mobile technology is exactly what the name implies – portable technology.¹

Mobile devices include:

- Laptop computers.
- Palmtop computers or personal digital assistants.
- Mobile phones and ‘smartphones’

In this day and age with picking up the notoriety of SMARTPHONES there is for all intents and purposes no distinction among COMPUTER and SMART telephones, so whatever Cyber Crime we knew about identified with Computers are likewise appropriate to Mobile Crime.

CYBER CRIME

Cybercrimes are those that are culpable under "Data Technology 2000" The easiest and least complex meaning of a "cybercrime" can be an illicit demonstration where a PC is a device or an objective or both. Lawbreakers can work secretly on a PC or any digital system.

Any individual who attempts to carry out a criminal behavior with a blameworthy aim or liable outlook he is called a guilty party or a digital lawbreaker. Cyber Criminals can likewise be youngsters and youths matured between 6 to 18 years. They might be programmers who can be named as expert programmers or saltines, disappointed representatives, or con artists.

¹Mobile technology Advantages and disadvantages of mobile technology Nifo business
<https://www.nibusinessinfo.co.uk/content/advantages-and-disadvantages-mobile-technology>
01/01/2020

MYSTIC INDIVIDUAL KIDS AND TEENAGERS (AGE BUNCH 9 – 16 AND SO FORTH)

This is extremely difficult to accept yet it is valid. The majority of digital wrongdoing lawbreakers we discover today are Teenagers. What they feel is of pride to have hacked into a PC framework or a Smartphone. These youthful understudies carry out digital violations without truly realizing that they are doing any unlawful movement.

Another explanation behind the expansion in the number of youthful crooks in are that a large number of the wrongdoers who are principally youthful school going understudies as they ignorant that hacking is wrongdoing, Professional hackers

Broad computerization has brought about business associations putting away the entirety of their data in electronic structure. Opponent associations utilize programmers to take mechanical insider facts and other data that could be advantageous to them. The impulse to utilize proficient programmers for modern undercover work additionally originates from the way that physical nearness required to access significant records is rendered needles if hacking can recover those.

SECTIONS OF IPC APPLIED²

SEC- 463 Forgery — Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury] to the public or any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

Sec- 464 Making a false document. — A person is said to make a false document or false electronic record— First —who dishonestly or fraudulently—

- (A) Makes, signs, seals or executes a document or part of a document;
- (b) Makes or transmits any electronic record or part of any electronic record;
- (C) affixes any [electronic signature] on any electronic record;
- (d) Makes any mark denoting the execution of a document or the authenticity of the electronic signature

² https://indiacode.nic.in/handle/123456789/2263?view_type=browse&sam_handle=123456789/1362

with the intention of causing it to be believed that such document or part of the document, electronic record or [electronic signature] was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly —Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with [electronic signature] either by himself or by any other person, whether such person is living or dead at the time of such alteration; or Thirdly —Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his [electronic signature] on any electronic record knowing that such person because of unsoundness of mind or intoxication cannot, or that because of deception practiced upon him, he does not know the contents of the document or electronic record or the nature of the alteration.

465. Punishment for forgery - Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

420. Cheating and dishonestly inducing delivery of property - anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

SIM CARD CLONING OFFENCE

In April 1988 this issue came into the picture when the Smartcard Developers Association (SDA) and two U.C.Berkeley scientists found a deadly cryptographic blemish in COMP128, the calculation that is utilized to ensure the personality inside the SIM that is utilized to secure the character of the SIM and to stay discreet verification key (KI) part secure.

The arrival of the security blemish revelation into the open area produced reports in the different media, all around the globe. Industry reacted to alleviate fears and console clients as for GSM's validation security. One suggestion mooted was that the time and cost it would take to clone

Versatile SIM card cloning is a digital offense where the safety information from one cell phone SIM card is replicated to another cell phone card. The other cell phone will turn into the precise or clone of the first telephone card. Versatile SIM card Cloning is otherwise called phone theft infringement and has been occurring in the vast majority of the created nations for decades. As of late, this wrongdoing has been found in our nation this is generally accomplished for making false

calls and messages. A duplicate of that unlawful SIM card can make calls and get messages from casualty's card and the charges for those calls and messages are charged to casualty's record

TODAY'S SCENARIO

In Today's reality versatile SIM card clients, regardless of whether it is Global System for Mobile correspondence (GSM) or Code Division Multiple Access (CDMA) risk having their telephones cloned and the most exceedingly terrible part is that there are not very many approaches to forestall this offense. At the point when we get or make calls from our telephone, the cloner can likewise tune in to those calls which we won't know about this offense. Although correspondence systems are outfitted with numerous security tests, yet cloners pull off the assistance of provisos in the telecom framework. So when one gets colossal bills, quite possibly the telephone may have been cloned

First Incident

In our nation cell phone cloning episode was first revealed in January 2005 when the Delhi Police captured a few people with 20 mobile phones, a PC, a SIM scanner, and an author. The blamed was running a trade where he was cloning sim cards to give modest worldwide calls to Indian foreigners in West Asian nations.

ESN/MIN data is not encrypted on the way to the MSC (Mobile Switching Centre) for further authentication. Thus, scanning the airwaves for this data is required if you wish to clone a phone card remotely. By changing ESN and MIN, the service provider will accept the call and bill it to either a wrong account. In order to ensure that it is a cellular phone and to forward billing information to that carrier

This issue is making a tremendous loss of valuable cash from financial balances of casualty as in our nation all bank exchange whether it is debit/credit card exchange or UPI PAYMENT or any OTP confirmation identified with the banking exchange system.

Cell phone cloning first started in telecom market since 1990's-mostly CDMA

- Started with Motorola "bag" phones.
- Motorola brick-
- Classic, model 800, ultra classic model phones of Motorola³

IN GSM technology it started from Europe and then moved towards other parts of the world

³ <https://prezi.com/nn6fisulkjfu/sim-cloning/>

CLONING WITHOUT HARDWARE OR PHYSICAL PRESENCE IN GSM PHONES

This incident was reported in July 2012 in **Lucknow**

As per the Times of India report as per reports, more than one Lakh sim customers have fallen prey to this new telecom fear assault as the recurrence of such calls keeps on developing. Knowledge organizations have apparently affirmed to the specialist co-ops especially in up west telecom division that such a racket isn't just underway yet the danger is developing quickly.

"It typically begins with a miss call from a number beginning with + 92. The second the customer gets back to on the missed call, their phone is cloned in the event that the endorser accepts the call before it is dropped as a miss consider then the guest on the opposite end acts like a call community official checking the network.

All progression of the specific specialist organization The guest on-call at other side at that point requests that the customer to press # 09 or # 90 get back to on his number to guarantee that the availability to the endorser was consistent," says a casualty who revealed the issue to the BSNL office at Moradabad a week ago. "The second I redialed that number, my record balance lost a total of cash from that point, in the three days that followed each time I got my mobile phone energized for levy, the parity would be diminished to single digits inside the following couple of moments,"

SIM CARD CLONING INCREASING BANKING FRAUD

Today we can't discover even a nationalized or state-level bank in our nation which doesn't give monetary exchanges endorsements through the cell phone and sim card. Security specialists state even though these are simple methods for causing an exchange however it can without much of a stretch make a major security break if your SIM or telephone is cloned. Your Smartphone has a duplicate of your spared information or your exchanges which could be effectively gotten to by digital crooks or fear mongers and utilized for problematic purposes.

OFFENCE REPORTED IN KOLKATA

Fraudsters have now begun utilizing cloned SIM for OTP exchanges which genuine monetary misfortune to casualty. Credit card fraud with the help of sim cloning in Kolkata

Somnath Sinha, a mid-level official at a Kolkata-based FMCG organization, was stunned when he got an SMS illuminating him in November a year ago that his credit card had been utilized to make

a Rs 45,000 buy. When he called his bank two hours after the fact to obstruct his card, it was past the point of no return.

He discovered that his cell phone had been utilized to demand a one-time secret key (OTP), which had been utilized to make the online buy. The bank would not remunerate him as the OTP demand had originated from his enlisted cell phone

SIM CLONING FOR FRAUDULENT CALLS IN DELHI

Delhi-based PK Sandell, previous specialized guide, UNIDO, He is A UNITED NATION ADVISOR saw his cell phone bill as bizarrely high. There was an abnormally high number of calls to numbers he was unable to perceive. Being qualified, he speculated that his SIM card had been cloned and was being utilized unlawfully by another person. This was affirmed when examinations demonstrated that a large portion of these calls was produced using the Chandni Chowk region, which he hadn't visited for a considerable length of time.

Fraudsters can without much of a stretch clone your versatile SIM card and get an association with your number. Dim market administrators in Gaffar Market in Delhi's Karol Bagh territory, Manish Market close to CST in Mumbai, and each unassuming community in Uttar Pradesh, Punjab and Rajasthan will "clone" any portable number of your decision for as meager as Rs 50-Rs 200. As there is a HUGE UNEMPLOYMENT issue individuals associated with this sort of wrongdoing to acquire income sans work and they carry out wrongdoing in our country.

Since numerous Customers utilize cell phones to get to their ledgers and get OTPs for their charge cards – and since spared passwords and other individual private Data can be gotten to by any individual who can utilize the important programming – this represents a genuine hazard to a huge number of supporters who, as Sinha and Sandell, can, conceivably, become survivors of extortion.

It likewise raises genuine national security chances as these telephones can be utilized for dread related correspondences and exchanges.

SIM CARD CLONING AND TERRORISM

Take the ongoing capture in the Philippines which depended on an objection by telephone mammoth AT&T. It was affirmed that a gathering of fear-based oppressors had hacked into telephone organizes in an offer to fund-raise which was purportedly utilized for the 26/11 assault on Mumbai. The four suspects purportedly focused on a framework called PBX frameworks.

Kept up by AT&T and accessed corporate telephone lines that they exchanged at a benefit to call focuses. The low-level trick came about in evaluated misfortunes of around 20, 00,000 US dollars Which means 12, 99, 30,000.00 Indian Rupee and happened between at any rate October 2005 and December 2008, and conceivably prior. This activity was conceivably financed by psychological oppressor association named Jemaah Islamiyah, a Pakistani fear based oppressor association which is accused of the psychological militant assault in Mumbai, India, in November 2008

TERRORIST USING SIM CLONING TO GENERATE FUNDS

Offshoots of fear monger association named Hizbullah cloned the mobiles of senior administrators of a Canada based telecom specialist co-op Rogers Communications, including boss executive Ted Rogers. Although the Firm had Technology set up to trigger alarms over dubious active call movement.

They were cloning the senior administrators more than once because "everybody was reluctant to cut off Ted Rogers' telephone," Hopper told Geffen, in a meeting that perceived the shrewdness of the social designing stunt. "They were utilizing truly splendid brain research," Said research by news agency

Background of Dispute

During the meeting, Hopper affirmed that Rogers had a framework set up Similar to those utilized by banks to hail up dubious card exchanges that were fit for spotting extortion in-progress. The data got by her accomplice empowered Drummond to record a little court guarantee against Rogers Wireless claiming that it "benefitting from wrongdoing" by neglecting to close down taken cell phones. Initially, Rogers resisted this action arguing that Drummond was responsible for calls made on the account before reporting that her phone was been misused.

However, after the news spread over the weekend, Rogers CEO Ted Rogers intervened and agreed to write off the debt along with covering the out-of-pocket costs for Geffen and Drummond

The trick just became visible after law teacher Susan Drummond tested a cell phone of C\$12,000 she got after she arrived from a month-long excursion to Israel. The MONSTER versatile bill recorded over 300 calls made in August to remote nations including Libya, Pakistan, Russia, and Syria. Drummond was advised she'd need to pay despite her fights than she'd never recently made abroad calls utilizing the record. Her ordinary bill was around C\$75.

On her ordered detailed bill she had discovered that calls had been made to Pakistan, Libya, Syria, and Russia when she was away.

An activity of this nature would viably mean calls and exchanges are being made by psychological militant gatherings under some other name which successfully ensures the character of the fear-based oppressor. In addition, they clone phones of conventional clients who are not being checked by insight offices.

Why cloning is easy for terrorist and militant organization-:

The procedure associated with telephone cloning is very straightforward for a fear monger. They record the Electronic Serial Number and the Mobile Identification Number before programming their cell phones to transmit MIN and ESN to their versatile system.

At the point when a call is then made by the genuine proprietor of the telephone, the data gets transmitted to the closest site and afterward, it stays on that site until it moves to the following site. This would mean on the off chance that you have been making a call from New Delhi in one charging cycle

You would be amazed to find in your bill that all the calls that have been made are from Bangalore or whatever other spots which these psychological militants have decided to call from.

SIM CARD CLONING LED TO MISTAKEN IDENTITY ARREST'S IN KIDNAPPING CASE

On April 4, 2016, the police strike on the entryways of Sameer Ahmed's home at Roshan Mohalla, Murudeshwar. The 19-year-old had recently given his pre-college tests and was anticipating the long summer occasions ahead. The police instructed him to go with them to the neighborhood Honnavar station and afterward instantly gave him over to a CID official. Sameer didn't know then that he would see his family just three months after the fact.

In what has all the characteristics of being an instance of mixed-up character, Sameer went through 90 days detained in Cooch Behar locale prison in West Bengal on the charge of seizing a young lady. It worked out that the real culprits had cloned his SIM card to lead the police off track. What's more, it worked for them.

CID official Sapna Ghosh, who secured his custody, said the arrest was made based on a habeas corpus filed by the girl's father alleging that he received a call from his daughter from the number belonging to Sameer. "After detailed questioning, I realized that it could be a case of SIM cloning,

and submitted before the court that Sameer is not involved, based on which he was bailed out,” Sapna Ghosh told The Hindu.

The Ahmed`s spent around Rs. 1 lakh (lawyer`s fees and other expenses) trying to get answers to their son`s arrest. Now that his summer break is over, Sameer hopes to return to college.

HYPOTHESIS OF PROJECT

The legislature has failed to frame strong and concrete laws for the offense of SIM cloning and TELECOM REGULATORY AUTHORITY OF INDIA or any other government body has not framed any guidelines to protect citizens from becoming the victim of this offense.

This Paper researcher would like to focus on suggestions to Increase security by enacting new legislation/regulations and which can cover the aspects of the highlighted topic. The researcher would like to suggest a possible solution in light of this issue and proper procedure of implementation of cybersecurity laws to ensure safety in light of increasing victims of SIM Card cloning in India today.

Thus the government of India and the telecom regulatory authority of India need to pay quick attention in filling the legislative vacuum in this area.

RESEARCH METHODOLOGY

Doctrinal research was carried out for research. Emphasis was given upon study of legal rules principles and laws governing cyber offenses Regulations of TRAI and department of telecom were studied related to this offense. News Reports of offenses Related to SIM cloning were studied and cases which were reported were analyzed

ISSUES AND POSITION IN LAWS

Status of Existing Laws to Protect Victims and Punishment for Criminals

The issue of information theft can be viewed as one of the significant focuses of lawbreakers in the present quickly evolving digital world and digital economic environment. This issue has neglected to stand out of legislators in our nation. Unlike different nations like the U.K which have their Data protection Act, 1984 for protection of their citizens.

There is no particular enactment or guideline in India to solve this Issue however India has its enactment called Information Technology Act, 2000 to address the consistently developing issues of digital wrongdoings, including information robbery.

The Truth is that our IT Act, 2000 is not complete or adequate to solve such crimes. The various provisions of the IT Act, 2000 which deal with the problem to some extent are briefly discussed below.

Can Theft of Data be Covered Through Indian Penal Code

Section 378 of the Indian Penal Code, 1860 defines 'Theft' as Whoever, intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property to such taking, is said to commit theft.⁴

Section 22 of IPC, 1860 defines "movable property" as "The words "movable property" is intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth."⁵

In any case, when we talk about sec 378 of Indian Penal code it just talks about "Portable Property" that is Corporeal Property, and Data is Intangible property and it isn't secured under the meaning of word "THEFT".

Be that as it may, if Data is put away in a medium (CD, Floppy, and so on.) and such medium is taken, it would be secured under the meaning of 'Burglary/Theft'. Be that as it may, if Data is transmitted electronically, for example in electronic form, it would not explicitly comprise robbery/theft under Indian laws as it is not an offense.

The best case of information in its immaterial structure can be contrasted with electricity. The inquiry of whether Electricity could be taken or not emerged arose before the Hon'ble Supreme Court in the case of Avtar Singh vs. State of Punjab (AIR 1965 SC 666). Responding to the above inquiry, the Supreme Court held that power is anything but a portable property, subsequently, isn't secured under the meaning of "Robbery" under area 378 IPC

However, section 39 of the Electricity Act extended Section 378 IPC to apply punishments with crimes dealing with electricity theft, so it became specifically covered within the meaning of the word "theft".

⁴ <https://indiankanoon.org/doc/1280620/>

⁵ <https://indiankanoon.org/doc/1439341/>

Position of Law in India

Currently, the mobile phone industry depends on basic laws of misrepresentation and robbery and in-house countermeasures to Track phone fraud and extortion cases. Mobile phone cloning is in the beginning stage of our nation.

Talking about the laws in our nation shockingly we don't have any to manage these kinds of offenses. SIM cloning as an offense has not been described in the IT Act of 2000. In any case, in 2008, mobile telephones were brought through the amendment in spite of the fact that there is no notice of SIM cloning in it.

With respect to penal provisions, there is no section for the Sim cloning offense.

Anyway Section 66 of the IT ACT could be applied which talks about extortion that is Done by Accused Indeed this is a bailable offense and whenever sentenced it endorses 3-year-detainment and a Rs 5 lakh fine which again is not an Obstacle for Accused

Position of Law in Other Countries

Phone cloning is restricted in the United States by the Wireless Telephone Protection Act of 1998, which prohibits "deliberately using, making, managing in, having control or care of, or having gear or application purposefully that it has been Used to insert or change media transmission distinguishing data related with or contained in a broadcast communications instrument so such instrument might be utilized to get broadcast communications administration without approval or consent of the owner.

Punishment under the wireless telephone act is 10 to 15 years. In the USA there is a federal communications commission to regulate telecom laws and Regulations

Cell Phone Cloning Process, Software's Used, Crimes Related and Safety Measures

Each SIM card has an exceptional Identity; the International Mobile Subscriber Identity (IMSI) is utilized to distinguish the client of a cell arrange and has a novel ID related to a particular cell coverage System.

SIM ID is put away as a 64 piece field and is transmitted from the telephone to the system. The Home Location Register (HLR) is privately replicated in the guest area register.

When turning on a cell phone, and when the telephone is turned on, the telephone enlists its SIM with the Operator system. The versatile system performs validation and approval against the HLR (Home Location Register) and imprints the IMSI as being dynamic. On the off chance that the

International Mobile Subscriber Identity (IMSI) is set apart as dynamic, the approval will fall flat, the system will prohibit the portable to get to its administrations. To make cloning effective we need to initially deactivate unique SIM cards.

Sim Card Cloning with Imsi Key⁶

STEP1 - Power your phone off and remove the back cover. Next, remove the battery from your phone. Remove the SIM card's carrier tray, and pop out the SIM card. Copy the IMSI (international mobile subscriber identifier) number. An IMSI is from eleven to fifteen digits long. The IMSI has imprinted on the SIM Card i.e. IMSI: 3211234567

Step2 - Now that you have the IMSI number you'll require the authentication key (KI), unique to your SIM. Use the SIM card reader that you will insert into the SIM card slot. SIM card readers can be purchased for around \$10 online.

Step 3 - Connect the SIM card reader to your SIM and your pc, the KI number will be retrieved and copy the entire contents. After the duplication is complete the new SIM will be identical to the old pop in the new SIM card and power your phone on to use.

How To Clone Sim Card Using Sim Cloning Tool

With just one click, the software collects all possible parts from the target device and generates comprehensive details on a computer that can be stored or printed.

Using Mobile Edit Forensic Software

Check the following steps:

Step 1: Download the software to your computer.

Step 2: Remove the SIM card from the device.

Step 3 Insert it to the SIM Card Clone Device and connect it to the computer.

Step 4: Run the SIM Clone tool from the main toolbar. The SIM Clone window will appear and you are ready to clone the SIM card.

⁶ <https://www.techwalla.com/articles/how-to-clone-a-SIM-card>

Step 5: Click on the Read SIM button to read the content of the original SIM card. The data will be read and you can choose which data you wish to copy.

Step 6: When the writable SIM card is inserted, the write SIM button will be enabled. Wait until the process is done.

Software used in this process used was mobile edit software of COMPELSON LABS (USA)

Cloning in CDMA Phones

For CDMA Cloning involved modifying or replacing the EP ROM in the phone with a new chip which would allow you to configure an ESN (Electronic serial number) via software. You would also have to change the MIN (Mobile Identification Number). When you had successfully changed the ESN/MIN pair, your phone was an effective clone of the other phone. Cloning required access to ESN and MIN pairs. Cloning is easy in CDMA phones as it takes a few minutes to clone any phone It has more success rate than GSM Cloning.

How to Know if Your Phone or Sim is Cloned

- 1- Frequent wrong number phone calls to your phone.
- 2- Difficulty in placing outgoing calls.
- 3- Difficulty in retrieving voice mail messages
- 4- Incoming calls constantly receiving busy signals.
- 5- Increased bill Amount.

Steps Taken by Telecom Companies to Detect Cloning in India⁷

According to economic times report published on 12 Feb 2012 Currently, none of the major telecom operators — Airtel, Vodafone, Idea, Reliance Communications and only Tata Teleservices can immediately track if two separate phones (one in the hands of a bona fide subscriber and the other being used by a fraudster with an illegally cloned SIM) are Simultaneously using the same number. This time lag (between the time the cloned SIM starts operating and this showing up in your telecom companies security system) provides frauds a long-enough window to complete their operations.

⁷ <https://www.hindustantimes.com/business/security-alert-frauds-can-clone-your-SIM-use-your-credit-card/story-cnstNfrpsdE5SSDA5YjkKK.html>

Steps Taken by Government⁸

In a meeting on September 3, 2013, the department of telecommunications (DOT) decided to set up a working group comprising representatives of the home and defense ministries and various national security agencies to draw up a blueprint to address loopholes in telecom security, including cloned SIMs. The industry will cooperate with the government in resolving it," added Pankaj Mohindroo, national president, Indian Cellular Association, the association of handset manufacturers. That's in the long term. Meanwhile, subscribers remain vulnerable to fraud.

The only way you can avoid becoming a victim is by remaining vigilant.

Steps to be Taken to Prevent Hacking

Some simple steps can be taken to prevent easy hacking of SIM cards. They may not completely prevent hacking, but somewhat reduce the SIM exploitation.

1- Better SIM cards

It is best for SIM vendors to use state-of-art cryptography with sufficiently long keys, should not disclose signed plain texts to attackers, and must implement secure Java virtual machines. While some vendors are upgrading their software, the others remain ignorant.

2- Handset SMS firewall

Additionally, handsets should be wrapped in a layer of protection and users to choose sources of binary SMS. An SMS firewall would also help.

3- In-network SMS filtering

SMS to phones should only be allowed from known sources but most networks have not deployed this level of filtering. Home routing is essential to customers when on roaming. This will protect the SIM from remote tracking.

Methods to Detect Cloning

- Duplicate detection
- Velocity trap
- Radio Frequency
- Usage profiling

⁸ <https://www.hindustantimes.com/business/security-alert-frauds-can-clone-your-SIM-use-your-credit-card/story-cnstNfrpsdE5SSDA5YjkKK.html>

- Call counting
- PIN codes
- Checking spam numbers in various applications like true caller

Duplicate Detection

- Same phone at several places at the same time
- Shutting down all of them
- A real customer will contact
- Cloned user switch to another clone

VELOCITY TRAP

- Mobile moving at impossible speeds
- Must be two phones with the same identity on n/w

USAGE PROFILING

- Keep customer phone usage profile
- Discrepancies noticed, customer, is contacted
- Example (local call OR foreign)
- Indicates a possible clone

PIN CODES METHOD

- To place a call, the caller unlocks the phone by PIN
- After the call completed, the user locks

How to Prevent Cloning

- Service providers have adopted certain measures to Prevent fraud, includes Encryption, blocking, blacklisting, user verification, traffic analysis.
- User verification using a PIN is one of the Customer verification methods
- Check that all mobile devices are covered by a corporate security policy
- Never hand over your SIM in physical form to another person Never allow any unknown person to Either make calls or receive calls using your SIM. Never give your personal information

through SMS or any other form to any other person. If you get a call from Telecom Company regarding your personal information, do not tell or reveal your personal information.

- Telecom companies do not need your personal information from time to time. Only at the time of giving out a new SIM, you would be asked for your personal information and that too with your signature. Remember not to give your personal information regarding your identity to any other person.

What can we do to protect ourselves from this Cybercrime?

We can develop new SIM cards with better technology that can never be cloned. Bad in the sense, with technically sophisticated thieves, customers are relatively helpless against cellular phone fraud. Usually, they become aware of the fraud only once receiving their phone bill

The latest technology that is available is PHONE PRINT introduced by a company named CELLULAR ONE.

Phone Print is a new technology that electronically fingerprints cellular phone calls, detecting and disconnecting calls made with stolen telephone numbers. This system will help to stop the fraud.

Just like your fingerprint, your call audio has a unique signature – a phone print. Whenever you pick up the phone, your device, your carrier, your geographic location, and your network routing contribute very subtle audio characteristics to your call. These traces of valuable information are invisible to most people – and it's important to note that, unlike your voice or your phone number, you can't manipulate, spoof, or otherwise disguise them.

Phone printing provides added security and helps detect fraudsters who are calling in. When a fraudster is detected, his or her phone print is added to a blacklist of "bad" callers. This blacklist is then used to compare with new incoming calls. Blacklists are populated when an enterprise confirms the phone print of a bad caller, and also through honeypot and research techniques that, for example, capture and then research calls made by fraudsters in mass phishing (phone phishing) attacks. About 70 percent of call center fraud is perpetrated by the same actors, so blacklisting their phone prints is a useful measure for stopping fraudsters in their tracks.

CONCLUSION

SIM cloning offense creates Loss for the subscriber who's SIM Card has been cloned. The person would face unnecessary legal complications. Hence there is an immediate need for an amendment to at least avoid such victims from being harassed unnecessarily and protect them from getting

cloned. It is therefore imperative that provisions for data theft be inserted in the IT Act, 2000 to extend the application of section 378 IPC to data theft specifically.

Weak legislations make our country more prone to cyber-attacks and where offenders move freely and again commit these activities. Financial loss due to mobile cloning. According to the cellular telecommunication industry association (CTIA), the financial loss due to mobile cloning is on the higher side in the United States. It is between \$600 and \$900 million. But in India it is in the initial stage, so the Indian government and network service provider can take preventive steps to control the frauds. According to hacker news, 2013 SIM card cloning hacking has affected 750 million users around the world.