Identity Theft As The Most Pervasive Form Of Cyber Crime: Its Socio-Legal Implications On The Indian Society:

Prof. (Dr.) Sonia Grewal Mahal
Professor in Law, Chandigarh Law College, Chandigarh Group of Colleges, Jhanjeri.

ABSTRACT
It is generally witnessed that there has been relatively little formal research on identity theft in India. Identity theft is a product of the revolution pertaining to Information Technology, and as such, it fits well into the literature of opportunity theory in criminology, which examines how criminals take advantage of new (and old) ways of doing business and conducting the affairs of everyday life in order to commit crimes. In this day and age of technical advancement, the crime of online identity theft has increased in frequency and severity. Despite the fact that this crime is not new, the Internet has broadened its scope and spawned new and inventive methods of committing it, resulting in a new version known as cyberspace identity theft. In order to steal someone's identity, the identity thief uses information about that person's identity such as their name, address, telephone number, maiden name, social security number, social insurance number, health card number, bank account information, driver's license number, and date of birth among other things. The Researcher through this present Research Paper has made a humble attempt to highlight the growing menace of identity theft in India and has also brought forth the socio-legal implications that the pervasive crime has in India. Also, an attempt has been made to bring forth certain relevant suggestions to fight this prevalent crime in India.

Keywords: Information Technology, State Legislation, Cyberspace Identity Theft, Socio-Legal Implications of Identity Theft.

INTRODUCTION
With the technological revolution, and with globalisation and digital adaptability now reigning across many industries, technology has had a rapid impact on people's mindsets. Information Technology's importance has risen to new heights, with both positive and negative consequences. Due to the development and revolution of Information Technology in India, identity theft has become a growing concern in recent years. In 1964, the term "identity theft" was coined. Identity theft has been defined as the theft of personally identifiable information since that time. Identity theft is the intentional use of another person's identity to gain financial, credit, or other benefits, as well as to harm or lose
another person. The person whose identity has been stolen may suffer negative consequences, especially if they are mistakenly blamed for the perpetrator's actions. A person's name, date of birth, social security number, driver's licence number, bank account or credit card numbers, PINs, electronic signatures, fingerprints, and passwords, as well as any other information that can be used to gain access to a person's financial resources, are all examples of personally identifiable information.

Despite the fact that the terms "identity theft" and "identity fraud" are legally distinct, they have become synonymous in popular usage. Identity theft is classified as a subcategory of identity fraud by several authorities. Identity theft is rarely a single crime, but rather a collection of several different crimes, many of which are well-known to the general public, if not all. Check and card fraud, various financial crimes, various telemarketing and Internet scams (Newman and Clarke 2003), theft of automobiles and auto parts facilitated by fraudulent documentation (Maxfield and Clarke 2004), thefts or robberies of various types in which identification information is stolen either accidentally or intentionally, counterfeiting and forgery, and human trafficking are all crimes that are frequently associated with identity theft (UNICRI 2003). The fact that victims were subjected to such a terrible crime prompted a series of congressional hearings that resulted in the passage of the Identity Theft Act of 1998.

Three important facts were brought forward for consideration: First and foremost, local law enforcement had been slow to recognise individuals as victims because the card issuer, rather than the cardholder, bore the brunt of actual financial loss, such as that arising from credit card fraud. In this case, businesses were seen as the victims rather than individuals. Second, the testimony of those who testified during the hearings revealed that their identities had been used for a long time until their usefulness had been depleted. They had, in reality, been the victims of a pattern of victimisation. Third, it was not uncommon for victims to discover they had been victimised some time after the fact, making an investigation into the crime more difficult.

"Identity theft results in at least tens of billions of dollars in losses," according to one conservative estimate. When we consider that annual losses from credit card fraud, insurance fraud, and health-care fraud amount in the hundreds of billions of dollars, and that identity theft accounts for a significant fraction of these crimes," this estimate may seem low. However, there is no way to estimate the amount of identity theft associated with these or other offences at this time.

The Secret Service estimated that the actual cost of identity fraud arrests in India was Rs.442 million, Rs.450 million, and Rs.745 million between 1995 and 1997; however, these costs included losses to victimised individuals and financial institutions and reflect the agency's focus on high-Rs. cases. The best estimate of the average cost of a financial crimes investigation in 2001 was Rs.15,000, although such instances vary so significantly that this figure is meaningless.

The Federal Prosecutor's Office in India in 2000, federal prosecutors prosecuted over 13,700 white-collar crimes at an estimated cost of Rs.11,400 per case — actual costs could be much higher or lower. Despite this, officials in several of the states contacted stated that current resources for investigating and prosecuting identity theft incidents are frequently insufficient. Police forces required to be properly trained in the complexities of identity theft investigation, in addition to the increased demand for prosecutors and support staff to prosecute cases. Furthermore, "police agencies are more likely to dedicate their limited resources to pursuing
violent crimes and narcotics offences than to complex identity theft cases that, even when successfully prosecuted, typically result in relatively low fines," according to the report. Despite the prevalent perception that businesses will carry the brunt of financial hardship, individual victims will incur costs.

According to a study, victims' average out-of-pocket expenses were between Rs.30 and Rs.2,000, however this amount does not include any legal fees. In this poll, the average loss to victims was Rs.808, but the majority estimated spending around Rs100 (Benner et al. 2000). The average amount of out-of-pocket expenditure for all types of victims was Rs.500, according to the Federal Trade Commission; however, the average amount of out-of-pocket spending for victims who opened a new account was Rs.1,200. Victims who discovered their information was being misused early on had a decreased chance of paying out-of-pocket costs. Those with household incomes less than Rs.75,000 were also more likely than victims with greater household incomes to pay out-of-pocket costs. The annual cost of identity theft to people, according to one estimate released by the National Fraud Center, is Rs.50 billion.

**MANY TYPES OF IDENTITY THEFT ARE AVAILABLE:**

**Financial Identity Theft:**
The most common methods are bank account and credit card fraud. Criminals may use a variety of tactics to perpetrate financial identity theft, such as opening a new credit card account in the victim's name, using the victim's Social Security Number and date of birth, and then exhausting the card's available credit. He then refuses to pay any bills, effectively making the victim a defaulter. The con artist may even change the victim's mailing address without regard for the charges. The imposter could even start a new bank account in the victim's name and write bounced checks. Financial and emotional stress are both experienced by the victim.

**Medical Identity Theft:**
This type of identity theft occurs when someone attempts to acquire medical supplies, prescriptions, or even submit false Medicare billings using another person's personal information, such as their name, medicare number, and so on. If this type of theft is perpetrated, it is possible that it may cause serious difficulties in the victim's life by disrupting credit scores and possibly causing inaccurate information to be recorded into the victim's medical records.

**Criminal Identity Theft:**
This is one of the most egregious types of identity theft, as well as the hardest to recover from. Instead, then just taking advantage of the victim's bank account, the thief assumes someone else's identity and uses it to commit crimes. When a thief is captured for a crime, he or she can get away with it if he or she provides a false self-identification during questioning by law enforcement personnel. The victim of this crime could face serious consequences as a result of the crime. To begin with, the victim could be served with an arrest warrant without his or her knowledge, putting him or her in jail. This would result in a lifelong criminal record, which would affect his or her future job, loans, and other financial commitments.

**Synthetic Identity Theft:**
This is the most common and serious sort of identity theft in today's world. Blending real information with made-up information is how a false identity is constructed. The fraudster may apply for credit cards, make purchases, and engage in a range of other activities in order to construct a financial history for this bogus identity. The consequence is a credit file that has been shattered as a result of Synthetic Identity Theft. When the thief uses a portion of the real person's SSN to establish a synthetic identity, the real person becomes associated with the synthetic identity because of the SSN used.

**Child Identity Theft:**
According to recent research, identity theft is a common crime that affects both adults and children. The most obvious reason for this practise is that underage children do not understand or recognise the importance of personal information. The juvenile becomes a victim of this crime when he or she reaches the age of majority and is able to use this information for official purposes. School forms frequently seek personal information about children, and parents should be aware of how their child's information is retained, processed, or even discarded to avoid any misuse.

**Drivers’ License Identity Theft:**
This type of thievery does not involve the application of certain fraud skills. In actuality, a criminal simply needs the victim's driver's licence, which may be obtained if it is lost or falls into the wrong hands. If the thief is caught speeding or otherwise involved in a transportation offence, this licence is either sold or used by the thief. As a result, the police will finally bring the true person to court, which may result in the person's reputation being ruined as well as financial issues.

**Tax Identity Theft:**
When a fraudster tries to file a tax return using another person's Social Security number without their knowledge, this is known as tax identity theft. The victim is fully unaware of this until he or she asks for a refund and discovers that a refund has already been requested using his or her Social Security number.

**REASONS AND MOTIVES FOR COMMITTING IDENTITY THEFT**
The types of identity theft are based on the offender's use of a variety of methods and motives. The sequence of actions or steps taken by offenders from the start to finish of their identity-related crime should be examined. Part of this has previously been accomplished by Lacoste and Tremblay (2003), who used a "script" method to analyse the processes and decisions made by check fraudsters while carrying out their illicit actions.

**Exploiting Weakness in Specific Technologies and Information Systems:**
The most well-known example of identity theft that targets a specific technology, notably the plastic card and its various qualities, is probably fraudulent use of a credit card (magnetic strip, hologram etc). The fraudster uses a variety of methods to tamper with or modify credit cards that have been stolen from victims or that have been counterfeited but have been attached to them with all of the victim's identifying information. Aside from the inconvenience of having
to apply for a new credit card and cancel the old one, the harm to the cardholder is likely to be minor. Nonetheless, using a credit card is a frequent method for thieves to convert stolen funds into cash or valuable items that they may then resell or re-sell.

Electronic databases that store personal and financial information about clients are also commonly targeted by this type of identity theft. Criminals have used some of this information to get access to bank accounts, obtain credit cards, open telephone or utility accounts, and then convert the stolen information into cash and other valuable assets. At this time, no examination has been conducted into the extent to which such databases facilitate the misuse of individual identities. The most well-publicized incidents of database theft have been those in which the culprits attempted to extort money from the companies or government agencies that manage the databases.

Financial Scams:
There are numerous forms of scams that can be used to obtain personal information from their victims. Identity theft of this nature is also linked to the misuse of specialised technologies and information systems. They're commonly utilised in telemarketing scams. On the internet, fraudsters create fake "shop fronts" that appear like well-known web stores, or they send phishing emails or pop-ups asking financial and personal information in the name of well-known retailers and, in many cases, government offices such as the Internal Revenue Service (IRS). In order to succeed, the vast majority of these types of fraud rely on tried and true old frauds that have been adapted to modern technologies. They all revolve around tricking or duping the victim in some way.

As Justification for Other Crimes:
Personal information about people now has monetary value, and criminals are aware of it. As a result, there is some evidence that offenders may commit traditional theft-related crimes with the primary purpose of obtaining personal information from their victims (Home Office 2004; "The Decline of The English Burglary," 2004). Burglary, robbery, muggings, auto theft, and pick pocketing are all crimes that can be committed with the goal of obtaining the victim's personal and financial information. Extortion or bribery may be used to get access to financial and personal databases or records maintained by corporations or other organisations, using threats or rewards for employees to reveal passwords or leave doors and cabinets unlocked, among other approaches.

Facilitating Other Crimes:
Theft of identification documents or fraud are the most common identity-related crimes used to commit other crimes. An expert identity thief will typically collect a few crucial pieces of information about a person's identity, such as their birth date and social security number, and use these to "breed" more documents in order to steal their identity. When skill fully employed over the phone, the Internet, in person with a bank official, or even when filling out a credit application, this information can aid in the acquisition of other information such as bank account numbers, driver's licence numbers, visas, and passports. The information might be used to produce new papers, such as counterfeit credit cards, which could include account numbers and names of legal account holders, making it more difficult to identify the cardholders. It is
feasible to obtain new credit cards and open new bank accounts. As a result, it is feasible to build a comprehensive business model and execute necessary transactions in order to engage in more illegal behaviour of a different kind.

To Avoid Arrest:
If an offender is apprehended, assuming another's identity can enable him or her escape being arrested or imprisoned, which is especially advantageous if the offender already has a criminal record or an active arrest warrant. When someone steals another person’s identity and commits crimes in that person's name, the authorities will go after that person rather than the real criminal, which could lead to a protracted inquiry.

Repeat Victimization: “Classic” Identity Theft:
In recent years, this type of identity theft has gotten the most attention. Despite the fact that the focus is on the victim's experience, the term "identity theft" refers to an offender's consistent and repeated attempts to use an individual's identity to generate money and provide opportunities for additional crimes until the identity's usefulness in generating money and providing opportunities for additional crimes has run out. Numerous victims have confirmed that this process occurs over a long period of time, but little research has been done to describe the process from the perspective of the offender, though some evidence suggests that experienced criminals who specialise in check and card fraud know how long to hold a card before turning it over to the authorities and when to dispose of the card in a public place (Mativat and Tremblay 1997).

Organized Identity Theft:
Offenders who are committed to their business are more prone to work in groups since the success of their schemes requires the participation of more than one person. Only a small amount of data on organised criminal behaviour involving identity theft is accessible, and the majority of it comes from studies of credit card fraud and identity theft (Mativat and Tremblay 1997; Newton 1994; Bury 1999:7; Steel 1995:16). Large-scale credit card theft necessitates a high level of competence, experience, and know-how. It also necessitates the establishment of a business that facilitates the sale of fake credit cards, all of which are required. At the very least, an organised crime group must achieve the following goals.

TECHNIQUES FOR PERPETRATING IDENTITY THEFT
Identity theft, according to the Black Law's Dictionary, is the illegal taking and use of another person’s identifying data for fraudulent purposes. Identity theft is a broad phrase that encompasses a wide range of activities ranging from misrepresentation to forgery. While some are considered traditional crimes, others, such as ATM skimming, phishing, and other forms of identity theft, fall under the umbrella of identity theft. Data theft and the acquisition of personal information through electronic devices can be accomplished through a variety of methods. The following are some of them:

Hacking
Hackers are unethical individuals that breach into other computer systems to steal information.
"Whoever, with the purpose or intention of causing any loss, damage, or destruction, deletion, or alteration of any information that resides in a public or any person's computer, diminishes its utility, values, or affects it injuriously by any means, commits hacking," according to Section 66 of the Information Technology Act of 2000. Hacking is a violation of one's fundamental right to privacy, as guaranteed by the Indian Constitution. It is a way in which viruses or worms, such as malware, divert information from another computer system by decrypting it and passing it on to a hacker, who then either uses the information themself or gives it to others to commit fraud with it.

**Phishing**
This method entails the use of forged email addresses or messages containing virus-infected websites. These infected websites entice users to provide personal information such as login credentials and account information, which is then utilised to perpetrate identity theft.

**Email/SMS spoofing**
The faked e-mail has an origin that is different from where it truly came from. In SMS spoofing, the perpetrator steals another person's identity in the form of a phone number and sends SMS via the internet, with the recipient receiving the SMS from the victim's cell number.

**ATM skimming/carding**
Cybercriminals make illicit withdrawals from an individual's bank account using ATM debit and credit cards.

**Vishing**
The cyber-criminal impersonates a bank representative or call centre staff and calls the victim, tricking them into disclosing sensitive information about their identity.

**Pharming**
Pharming is a type of online fraud that involves malicious code and fake websites. Cybercriminals install malicious code on a computer server through this method. Without the user's knowledge or consent, these programmes automatically redirect the user to fraudulent websites. Users may not detect the fraudulent behaviour while providing personal data and information, as well as financial data, on these websites since they look similar to the legitimate website.

**Malware**
Malware is malicious software that is meant to harm or destroy computer systems and their data in order to gain unauthorised network access. Viruses, ransomware, and spyware are examples of malevolent software types. Malware is often distributed via email as a link or file, requiring the user to click on the link or open the file in order to run it.

**LEGAL FRAMEWORK TO CURB THE MENACE OF IDENTITY THEFT IN INDIA:**
According to the Indian Law, identity theft is considered to be punishable under two legislations, namely:
a) The Indian Penal Code (IPC), 1860, and
b) Information Technology Act (IT Act), 2000.

After the Information Technology Act of 2000 amended the Indian Penal Code, identity theft was recognised as a crime. These new provisions are primarily concerned with electronic records. According to the IPC, 1860, an electronic record is defined as "data, record, or data created, image, or sound sent or received in any electronic form," which is comparable to the description given in the IT Act, 2000.

The Indian Penal Code (IPC)
Section 378 of the Indian Penal Code (1860) may not include identity theft because it only applies to movable, tangible goods and excludes internet. Although no explicit section of the Indian Penal Code, 1860, mentions "identity theft," Sections 463, 464, 465, 469, and 474 of the IPC, 1860, have provisions for punishing forgery, and identity theft has now been added to the ambit of these provisions following the modification of the IPC, 1860. Identity theft is defined as cheating under sections 419 and 420 of the IPC, and is equally punished, while cheating through impersonation is dealt with under section 417. The Indian Penal Code of 1860 makes identity theft a crime, classifying it as a more serious kind of forgery or deception.

The Information Technology Act of 2000
After being amended in 2008, the word "identity theft" was introduced to the Information Technology Act of 2000. It took some time to grasp the importance of offense-specific legislation, such as Section 66 C of the Information Technology Act of 2000, which safeguards the fraudulent and dishonest use of any person's identification feature. Another major stumbling block on the path to justice is the implementation and enforcement of these laws. In India, there is no personnel to deal with the continuously evolving cybercrime. Also contributing to the surge in the number of occurrences of identity theft is a lack of awareness of these major cyber-crimes.

The National Cyber Security Procedure (NCSP) of 2013 focuses on the establishment of a National Nodal Agency as well as the implementation of a proper and stringent certification policy. There is now just one form of certification policy under the IT Act of 2000, namely ISO027001 ISMS certification, which does not meet the legitimacy of such certification, and NCSP has no plans to develop more certification policies. The NCSP, published in 2013, also supports adherence to open standards and the use of public key infrastructure. In addition, the policy plans to establish a team of roughly 5 lakh people in the next five years, which will fall short in reality. Overall, the National Cyber Security Policy of 2013 turned out to be a flimsy concept that was far off from reality. Thus, these rules appear to be competent in combating the crime of identity theft; nonetheless, the increasing number of reported cyber breakouts raises various concerns about the existing legislation.

IDENTITY THEFT IN INDIA: SOME CASE STUDIES

CBI Vs Arif Azim [(2008) 105 DRJ 721; (2008) 150 DLT 769]

In this example, Sony India ltd operates a website called www.Sony.Sambandh.com, which allows NRIs to make online payments and have Sony products delivered to anyone in India.
The payment was made with a credit card that was used by an American citizen to deliver a television and headphones to Arif Azim, a resident of Noida. After all of the legalities and delivery were completed, the credit card company informed Sony that the card owner was disputing the payment, and Sony filed a fraud complaint with the CBI. Arif Azim, a call centre employee, was later discovered to have obtained the card user’s information and utilised it to order merchandise using that information. The company reported internet cheating to the Central Bureau of Investigation, which opened an investigation under Indian Penal Code Sections 418, 419, and 420. Arif Azim was detained once the case was examined. Arif Azim obtained the credit card number of an American national while working at a call centre in Noida, which he exploited on the company’s website, according to investigations. In this one-of-a-kind cyber fraud case, the CBI retrieved the colour television and cordless headphone. The CBI had enough evidence to prove their case in this case, thus the accused accepted his guilt. Arif Azim was found guilty under Sections 418, 419, and 420 of the Indian Penal Code, marking the first time that cybercrime has been found guilty.

**NASSCOM v. Ajay Sood and Ors,119 (2005) DLT 596.**

In this landmark decision, the Delhi High Court deemed online phishing to be illegal, resulting in an injunction and damages recovery. In order to set a precedent in India, the court defined phishing as a type of computer fraud in which a person impersonates a genuine organisation, such as a bank or an insurance company, in order to steal personal data from a customer, such as access codes, passwords, and so on. Personal data obtained by misrepresenting the identity of the lawful party is frequently exploited for the benefit of the collecting party. The Court further remarked, as an example, that common phishing scams involve people impersonating online banks and stealing money from e-banking accounts after duping customers into turning over private financial information. The National Association of Software and Service Companies (Nasscom), India’s top software association, was the plaintiff in this lawsuit. The defendants ran a placement firm that specialised in headhunting and recruitment. The defendants created and sent emails to third parties in the name of Nasscom in order to gather personal data that they could utilise for headhunting reasons. The plaintiff’s trademark rights were recognised by the High Court, which issued an ex-parte ad interim injunction prohibiting the defendants from using the trade name or any other name that is confusingly similar to Nasscom. The defendants were also barred from claiming to be affiliated with or a part of Nasscom, according to the court. A commission was established by the court to search the defendants’ homes. The local commissioner assigned by the court took custody of two hard drives from the machines from which the defendants sent false e-mails to various parties. The incriminating emails were subsequently extracted from the hard drives and presented in court as evidence. During the course of the cyberlaw lawsuit in India, it became obvious that the defendants, in whose names the infringing e-mails were sent, were false identities constructed on the defendants’ orders by an employee in order to evade detection and legal action. Following the discovery of this deception, fictional names were removed from the list of defendants in the lawsuit. Following that, the defendants admitted to their illegal actions, and the parties reached an agreement by recording a compromise in the court proceedings. According to the terms of the settlement, the defendants agreed to pay the plaintiff Rs1.6 million in damages for infringement of the plaintiff’s trademark rights.

570 http://www.webology.org
CYBER ATTACKS IN INDIA

Cyber Attack on Cosmos Bank
In an exceptionally aggressive cyber-attack in August 2018, the Pune branch of Cosmos Bank was robbed of Rs 94 crores. By breaking into the main system, the attackers were able to transfer the funds to a Hong Kong bank. In addition, the hackers gained access to the ATM server in order to obtain information about numerous VISA and Rupay debit cards. The switching system, which connects the centralised system to the payment gateway, was hacked, which meant neither the bank nor the account holders were aware of the money transfer. According to the international cybercrime case study, a total of 14,000 transactions were carried out using 450 cards across 28 countries. A total of 2,800 transactions were completed across the country using 400 different cards. This was the first malware attack of its kind, and it effectively shut down all communication between the bank and the payment gateway.

UIDAI Aadhar Software Hacked
A massive breach of personal data affecting approximately 1.1 billion Indian Aadhar card holders occurred at the start of 2018, signalling a dramatic start to the year. The UIDAI (Unique Identification Authority of India) announced that the details of Aadhar have been exposed online on around 210 government of India websites. Not only Aadhar records are disclosed online, but also PAN and mobile numbers, bank account numbers, every personal information of individual card users, IFSC codes, and so on. Along with this, another story rocked the nation, claiming that unknown marketers were selling Aadhar information for Rs.500 on WhatsApp. Also, if a person wants a printout of someone's Aadhar card, they must pay an additional Rs 300.

Hack Attack on Indian Healthcare Websites
Recently, in 2019, India's healthcare websites caught the attention of cyber attackers and became one of the victims of these attacks. According to reports from US cyber security organisations, hackers first broke into the website and then entered India's leading healthcare website. Hackers were able to obtain the personal information of around 68 lakh patients and doctors as a result of this attack.

SIM Swap Scam
Two hackers were arrested in Navi Mumbai in August 2018 for transferring 4 crore rupees from various bank accounts, according to reports. They fraudulently transferred money from a number of people's bank accounts. Both attackers were successful in blocking SIM cards for a number of people after fraudulently gaining access to their SIM card information. All of the transactions were done through online banking with the use of forged documents. They also attempted to hack into the accounts of a number of well-known companies.

TECHNIQUES TO REDUCE IDENTITY THEFT
Situational prevention divides up the possible techniques into five categories:
• Increase the effort the offender must make to complete the crime
• Increase the risks of getting caught
• Reduce the rewards that result from the crime
• Reduce provocations that may encourage or otherwise tempt offenders
• Remove excuses that offenders may use to justify their crime

CONCLUSION:
A variety of study opportunities were discovered as a result of the identity theft. To date, it is clear that the FTC has done or commissioned the only scientifically valid studies. Because the FTC's objective is to safeguard consumers, it's inevitable that the attention will shift to victims and the impact of identity theft on consumers. As a result, the involvement of local police departments in reporting and recording identity theft becomes increasingly important. The focus on police insensitivity to individual victims' anguish has been observed to come from the media attention around several high-profile cases, which was bolstered by subsequent congressional investigations and legislation.

Although much progress has been made in teaching police officers to recognise and respond to victim suffering in such cases, it must be emphasised that the emphasis on police response is based on anecdotal evidence and a few studies with small sample sizes and other methodological flaws. As a result, determining the percentage of victims who are actually victims of identity theft, as opposed to those who may merely experience little inconvenience, becomes even more important. While the FTC data provides some insight, it is mostly based on consumer and victim reports rather than actual police activity. As a result, there should be a better connection between victim-centered research and research on the real criminal justice response to identity theft.

Installing and upgrading cyber security systems is a wise investment in the future prevention of cybercrime. Furthermore, in order to prevent such cyber criminals, the law must be strictly enforced and in its entirety. Furthermore, to avoid identity theft in the first place, preventative measures must be taken. A problem as large as identity theft, which is a result of the information society's increased opportunities for criminals. Rather than settling a huge number of little or even major crimes, the police might profit from focussing their resources on preventative measures. However, it is unreasonable to suppose that police can address all of the elements required to reduce criminals’ chances on their own. They need help from a variety of institutions that contribute to the problem, including credit reporting agencies, retail stores, and banks, to mention a few. All organisations who issue identification paperwork or must authenticate identities as part of their operations are also required to help. Identity theft prevention partnerships may be developed, and the government's role in supporting such partnerships could be critical in bringing identity theft under control. Furthermore, we believe that when looking for effective interventions, research should focus on specific acts of identity theft, rather than lumping together the various behaviours that are usually grouped together and classified as "identity theft." The statistics and terrible events of recent cyber-attacks in India are a warning signal and a wake-up call for every individual, Corporation and Government to update their cyber security systems to defend themselves and for the proper implementation of the Laws relating to it with a strong hand to curb the criminal activities of the cyber criminals.
References: