Dama International Journal of Researchers (DIJR), ISSN: 2343-6743, ISI Impact Factor: 1.018
Vol 2, Issue 8, July, 2017, Pages 11 - 21, Available @ www.damaacademia.com

Critical Evaluation of Identity Theft as E-Transactions Fraud for New Dynamic Regarding Legal Remedies

M'Bia H. De-Yolande, PhD. Candidate

China University of Political Science and Law, Beijing, Xitucheng Road, N0. 25,100088.

Email: oreargent@yahoo.fr / Corner333stone@yahoo.com

I. INTRODUCTION

No one has a franchise when it comes to online identity theft fraud. Fraudsters tempt us all regardless gender, age or association. Be it online or off line fraudsters known how to use our own interests against us. At a given moment, everyone may have undergone that fraud scheme, experienced online identity theft. Identity theft statistics and examples have been some of the most prevalent forms of e-transactions fraud between 2012 and 2016[1]. As a matter of fact, transactions conducted by electronic means have given rise to various frauds. Among these identified online fraud schemes is identity theft which presents two-fold category: The first is referred to as 'True name'[2] in which the thief of identity utilizes a third person personal data to open various accounts and even registers for services or makes online purchases The second type is Account takeover"[3].As the name illustrates, information gathered from an illegal access to a computer is used to log into existing accounts and engage into electronic transactions in someone's name. Both are very serious, and can result in significant financial loss as well as emotional distress.

According to the Organization for Economic Co-operation and Development(OECD), identity theft ''occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorized manner, with the intent to commit, or in connection with fraud or other crimes.''[4] Here someone fall for a phishing scam after following a link within a personal e-mail fearing to avoid apparent suspension of his account by replying to an e-mail that appeared to be in relation to his bank account. The personal details once entered as requested make realize that a certain amount of money had been withdrawn from the personal account. There someone had failed to update the internet security software only to discover later that malicious software had taken control of the computer and sent bogus e-mails to close relatives, friends and acquaintances that included a link to further spread the malicious code. The personal information retrieved afterward from the computer is generally used by fraudsters to register for several credit cards and sign up to a number of purchases on E-transactions sites. This is how identity theft works and much more schemes to add to the collection when associated with other e-transactions frauds.

Surprisingly despite the existing laws to curb the scourge, online identity theft remains unabated. Not only the number of victims' has experienced a rise throughout years but also the fraudsters find the way to cover their tracks and escape the law, putting at trial law enforcers, those in charge of investigations for what matters and policyholders. There are many ways in which identity theft may occur. This study examines factually two methods, to wit, identity theft that involves the use of credit cards and virtual currency as a tool to conceal proceeds of international fraudulent online identity theft activities.

States agree that it is a problem that needs to be dealt with both domestically and internationally. However the fact that ID theft is referred to as a crime, a fraud, an aggravated fraud, a serious crime or even a cybercrime does not help to harmonize the legal measures. This circumstance will be difficult to manage especially in cross-

---

[1] *Valuable Statistics About Identity Theft you need to know, https://www.idtheftauthority.com/identity-theft-statistics-2016/. November 11, 2016, accessed March 15 2017.*

[2] *''Why is Identity Theft a Threat?. Available at http://www.bullguard.com/zh-cn/bullguard-security-center/internet-security/internet-threats/why-is-identityt-theft-a-threat.aspx ,2017 BullGard; Accessed February 14,2017*

[3] *Ibid*

[4] *OECD Observer,oecdobserver.org, No 268,June 2008;Accessed December 27,2016*

border e-transactions fraud cases that mainly necessitate outside border investigations; and the reality is that with the development of technology such cases happens at a high frequency in E-transactions fraud. This study therefore proposes a new dynamic to consider in terms of remedies to the victims in order to address the matter but more importantly to assist the victims seeking compensation after being defrauded. We believe more stringent compensation regime which will serve as deterrence are more than necessary.

II. IDENTITY THEFT IN E-TRANSACTIONS

Define Identity Theft is the first step to better understand how it works and to what extent it has spread throughout the years.

A. Identity Theft vs. Identity Fraud

Is Identity theft, identity fraud, interchangeably or do they follow different paths? Both the terms that are often used interchangeably indeed, though, identity fraud is the broader term that refers to a number of crimes involving the use of false identification, therefore not necessarily means of identification belonging to another person[5]. On the other hand, Identity theft is defined as the specific form of identity fraud that involves using out of legal basis the personally identifiable information of someone else.[6]

Both identity theft and identity fraud are often committed in connection with other violations.[7] Identity theft however may involve an additional element of victimization, as this form of fraud may directly affect the life of the victim whose identity was stolen in addition to defrauding third parties[8].

A definition that encompasses both terms defines Identity theft and identity fraud as referring to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception and typically for economic gain.[9] For the purpose of our study we will use identity theft/thief.

Further in 2009 the case Flores-Figueroa vs. United States brought a clear understanding between identity theft and aggravated identity theft.[10] The Court decides that in order to be found guilty of aggravated identity theft, a defendant must knowledge that the means of identification he used belonged to another individual. It not sufficient to only have knowledge that the means of identification used was not his own.

B. Identity Theft Worldwide Statistics

Personal information such the date and place of birth, address, social security number or information about your job may be impersonating you and being used without your knowledge to do transactions in your behalf such as buy products and services; ask for loans and obtain credit cards, transfer someone bank balance; monitor financial accounts or create new ones; obtain of passports, visas and other important files or documents. Etc.

In Australia identity theft, in particular, poses a significant financial cost to the community with estimates ranging from $2 billion to $3.5 billion a year according to the Australian Institute of Criminology[11]. In 2015, there were

---

[5] *Kristin Finklea, Identity Theft: Trends and Issues; Congressional Research Service Report, January 16,2014,P.3*

[6] *Ibid*

[7] *Identity theft is often associated to credit card fraud*

[8] *Such as the governments, employers, consumers, financial institutions etc..*

[9] *See supra note 143*

[10] *Flores-Figueroa Vs. United States, 129 S.Ct.1186 (2009)*

[11] *Milind Sathye, Eugene Clark and Anni Dugale, Fraud in E-Government Transactions: Risk And Remedies, future Challenges for Government-Privacy and Legal; Discussion Paper no.14,*

more than 148,000 victims of identity theft in the UK compare to 94,500 in 2014 with 85% of the fraud carried out online.[12] In Canada and United States, many reports showed that unauthorized persons have taken funds out of a third person bank or financial accounts[13].In the worst cases, victims' identities are used running up vast debts and committing crimes.

Unfortunately, the impact of identity theft is not solely financial. In many cases a victim's losses may include substantial additional financial costs associated with trying to restore his reputation in the community and correcting erroneous information for which the fraudster is responsible.[14] Due to its impact identity theft is one of the unlawful acts regulated by the majority of countries. However the development in the means of committing, to wit, the fact that identity theft is often used to perpetrate other frauds need a closer look and more importantly higher remedies take into account not only the financial aspect but also the emotional recovery for the victims' benefits.

To go further, in July 2016, Cifas, the UK's leading fraud prevention service, released new figures showing a 52% rise in young identity fraud victims in the UK[15] with significant increase in Manchester (83%), London (78%) and Leeds (59%). In 2015, 24,000 (23,959) people aged 30 and under were victims of identity fraud. An increase of 15.766 is observed compare to 2014 and 2010 that summed up 11,000 victims of same age bracket. Fraudsters have found in the youth interests for new technologies materialized in the possession of smart devices and in online shopping that expose their individual information, the opportunity to target them and conduct large scam operations. Plus, a short film, used as an advertisement filmed in a London coffee shop ''Data to Go'[16]' launched online, uses hidden cameras to capture astonished reactions from people caught in a stunt where their personal data, all found on public websites, is revealed to them live on a coffee cup. The film ends with the line ''don't make it easy for fraudsters. Set your privacy settings''. It intends to raise awareness about ID theft. Education about E-transactions fraud is useful to prevent potential fraud attempts but it not sufficient for legislation play the primary role. Additionally South African Fraud Prevention Services reports that it is likely that the country loses Rand 1 billion a year because of identity theft.[17] The two types of identity theft which appear to be on the rise in the country are phishing scams and hacking attacks.[18] Likewise the US Federal Trade commission (FTC), in 2006 for the sixth year in a raw, identity theft topped the list of consumer complaints, accounting for 246,035 of more than 674,354 fraud complaint filed with agency[19] and is still on the rise despite the regulations.

---

[12] Identity fraud up by 57% as thieves 'hunt' on social media; bbc.com; July 5,2016;Accessed December 26,2016

[13] The United States Department of Justice, Identity Theft,justice.gov, December 2,2016, Accessed December 26,2016

[14] In one notorious case of identity theft, the perpetrator, not only caused more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name, but called his victim to taunt and scoff him saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time before filing for bankruptcy, also using the victim's name. While the victim and his wife spent more than four years and more than $15,000 of their own money to restore their credit and reputation, procure a firearm, but made no restitution to his victim for any of the harm he had caused.

[15] Cifas, Criminals Target UK Youth As Identity fraud Rises. Available at https:// www.cifas.org.uk/press_centre/criminals_target_UK_youth_as_dentity_fraud_rises,2017Cifas.Last visited February 14, 2017.

[16] About the short film-advertisement, the framework is weaved as follows: with the promise of a free coffee and a croissant, participants were asked to 'like' the café's Facebook page. A team of background researchers, within a maximum time period of three minutes, searched across public websites to find as much personal information and data as possible. That data was then radioed through to a barista, who wrote it on to a cup and handed it to the unsuspecting customer. Hidden cameras captured their 'baffled' reactions.

[17] VREPORT, Identity Theft 'Costing SA Millions;v-report.co.za; Accessed December 27,2016.

[18] Identity Theft escalates in SA, July 9th,2015.enca.com;Last Visited December 27,2016

[19] Ibid

The least we can say is Identity theft has generated substantial economic losses for stakeholders, including individual victims, financial institutions and even whole economies. In the UK for example, the Home Office estimates that identity fraud costs UK GBP1.7 billion, equivalent amount of (US$330 billion) to the Uk economy.[20] Besides In January 2012 results of a survey by the National Fraud Authority (NFA) of more than 4,000 UK adults online revealed that 9.4 per cent had been an identity fraud victim in the previous 12 months. The overall estimated Individual loss from identity theft amounted £1.2 billion[21].The figures accentuated above prove that ID theft is unabated. Only more stringent remedies could reduce the scourge.

III. IDENTITY THEFT COMMITTING MEANS

A. Common Types

The rise of Smartphone and tablet penetration in Southeast Asia has caused in the region the increment of the phenomenon of ID theft. 62 percent of internet users in Indonesia and 41percent in Thailand use only smartphone to connect compare with 11 and 6 percent respectively in United States and UK. In addition, 37 percent of Singaporeans and 32 percent of Malaysians made their latest purchase online[22] while shopping and entertaining services, as well as public services, increasingly move online, education and awareness about online privacy and safety remains law. More people are routinely sharing data loosely with organizations than ever, and through insecure channels, putting personal information at risk more than ever.

It has been revealed that most victims of ID fraud are not aware that they are victims until it is too late[23] until a bill arrives for something they did not buy or they experience problems with their credit rating. To carry out this kind of fraud successfully, fraudsters usually have access to their victim's personal information such as name, date of birth, address, their bank and the different accounts subscribed to. Fraudsters get hold of this in a variety of ways, including through hacking and data loss, as well as using social media to put the pieces of someone's identity together. 86 per cent of all identity theft in 2015 was perpetrated online.

The sophistication level of professional ID thieves involved in organized transnational groups continue to grow along with the methods they develop[24] From individually tailored phishing and fishing scams[25],to increasingly successful hack of corporate and governments databases, to elaborate networks of bonnets designed to hijack millions of computer without any trace[26]. Seven percent of smartphone owners are impacted by ID theft since 62 percent of them do not use a password on their home screen and 32 percent save log-in information on their devices and with the advancement of technology anyone can download free Apps to turn the phone into a credit card skimmer in order to commit fraud.[27]

Moreover, according to Cifas, the UK's leading fraud prevention service Chief Executive ''…Facebook, Twitter, LinkedIn and other online platforms are much more than just social media sites they are now a hunting ground for

---

[20] *Action Fraud, Fraud Cost the UK over 73 billion, says the National Fraud Authority; http://www.actionfraud.police.uk/fraud-costs-the-UK-over-73-billion-says-National-Fraud-Authority-Mar12 March 29.2012, Accessed February 14, 2017.*

[21] *Ibid*

[22] *Edwin Seo, Identity theft going viral in Southeast Asia, enterprise innovation.net, May 25;2015*

[23] *CPP IDprotect ''How do I know if I am a victim? cppasia.com.sg; June 2014,accessed February5,2017*

[24] *Identity Theft and Scam Prevention Services: Identity Theft Victims Statistics; identitytheft.info 2007-2017.*

[25]*See section 2.3 on Phishing: The full extent of the Problem.*

[26] *Supra note 243*

[27]*Identity Theft Statistics show increasing global issue,armourcard.com; Accessed December 26,2016*

identity thieves''[28]. Indeed, the data taken from 261 companies in the UK suggests fraudsters are increasingly getting personal information from social media sites such as Facebook, Twitter and Linkedln[29] or Sina Zeibo and Taobao in China[30] to gather information about someone's identity; thus highlighting the need to be savvy when filling up privacy settings online.

In China, personal information may be purchased by category or in what is called an ''11-type information package''[31] which contains flights numbers, phone numbers, hotel check-in records to bank account transaction statements with a person's identification card number. The package online price is about 700 Yuan (about 101 USD).[32] The delivery takes 2 days after the purchase[33]. The perpetrators also offered services such as tracking down bank balances with ID numbers and positioning one's specific location within with a phone number at the price of 600 Yuan. This circumstance led to the Ministry of Public Security to consider criminalize acts such as illegally obtaining personal information by theft, purchase or any another methods.[34]

Inversely, technology-may also evolve as helpful means to combat online ID theft. In Korea, in 2006, an improved online identity system was introduced. The 13- digit citizen registration number, which contained people's personal information and was used as an online ID verification tool, was replaced by a new "i-PIN" (Internet-only Personal Identification Number) with no personal data, which could be replaced if copied or misused, and which could not be used to trace other website registration information. Despite the utility of modern technology to deter ID theft perpetrators, it is worth noted that only the law offers a sustainable and reliable solution to the problem. Meanwhile, basic methods of ID theft continue unabated. From stealing wallets and purses, to the use of pretext and social engineering to deceive customer call centers into releasing personal accounts information, the original methods of identity theft still work. No doubt, Internet has become an appealing place for fraudsters to impair E-transactions. Obtain identifying data, such as passwords or even banking information come as easy as a shopping online that demands not much than a few clicks. In their haste to explore the exciting features of the Internet, many people respond to "spam" which are unsolicited E-mails, all designed to fool people into disclosing their personal information. At this stage, many people do not realize how easily criminals don't need to break into households to obtain personal information. Also they have their own ways in public places for instance criminals may engage in slight physical contact such as ''shoulder surfing''[35] stumble into you or observing you from a nearby location as you punch in your telephone calling card number or credit card number; listen a conversation you are engaged in if you give your credit card number over a phone to a hotel or rental car company; in other words in casual moments daily life situation. If you receive applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, fraudsters may retrieve them and try to activate the cards for their personal use.

---

[28] *Cifas, Criminals Target UK Youth As Identity fraud Rises. Available at http:www.cifas.org.uk/press_centre/criminals_target_UK_youth_as_identity_fraud_rises. Cifas 2017; Last Visited February 14, 2017*

[29] *Identity fraud up by 57% as thieves 'hunt' on social media; bbc.com, July 5,2016,Accessed December 26,2016*

[30] *gbtimes, Online Identity Theft Crackdown begins in China,gbtimes.com, December 13,2016,Visited December 26,2016*

[31] *China Radio International, Online Identity Theft crackdown begins in China, gbtimes.com; December 13,2016.Accessed December 27;2016*

[32] *Ibid*

[33] *Ibid*

[34] *China Radio International, Online Identity Theft crackdown begins in China, gbtimes.com; December 13, 2016.Accessed December 27; 2016.*

[35] *Ibid*

As a consequence, some credit card companies, when sending credit cards, have adopted security measures that allow a card recipient to activate the card only from his or her home[36] telephone number.

Also, if your mail is delivered in a public access computer, fraudsters may as well intercept and redirect the electronic mail to another location.[37]

B. Trend: Hands-Free Pickpocket

Identity theft is a costly unlawful act that affects millions of people worldwide[38]. Both victims and offenders come from all demographic groups. Typically, the types of crimes that fall under the identity theft umbrella include new account fraud(where fraudsters create new bank and credit card accounts in the victims' names); existing non-credit card account fraud(where the offenders take over existing financial accounts), and existing credit card account fraud(where fraudsters use the credit card numbers of their victims).[39]

Identity Theft Resource Center [40]sub-divides identity theft into five categories: Criminal identity theft (posing as another person when apprehended for a crime); Identity cloning (using another's information to assume his or her identity in daily life); Medical identity theft (using another's identity to obtain medical care or drugs); Child identity theft (occurs when a minor's identity is used by another person for the imposter's personal gain. Social Security numbers of children are valued because they do not have any information associated with them. Thieves can establish line of credit, obtain driver's licenses, buy a house; can go undetected for years, as most children do not discover until years later. Child identity theft is fairly common, and studies have shown that the problem is growing. Financial identity theft appears to be the most common type when someone wants to gain financial benefits in someone else's name. This includes getting credits, loans, goods and services, claiming to be someone else.[41] According to the inaugural MasterCard Safety and Security Index, consumers across Southeast Asia and china cited identity theft and ATM-related fraud as the top two security concerns when it comes to electronic payments.[42] Indeed 42 percent of consumers in Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam were most concerned with ATM-related fraud such as a stolen card, card cloning or skimming. In the Greater China markets (Hong Kong; China and Taiwan), this figure was 31 percent.[43]

In hands-free pickpocket scheme thieves can steal credit card information through a technology called Radio Frequency Identification (RFID), which uses radio waves[44].The digital pickpocket randomly brushes a device called a skimmer close to someone's purse or wallet and steals the information from the cards inside. It takes merely a second for the information to be overlaid onto any card with a magnetic strip and used to make purchases.[45] It doesn't take much to leave one's personal information on social sites for fraudsters to look after and misuse it, but the hand-free pickpocket shows the possibility for everyone to get robbed any time at any place

---

[36] *CPP IDprotect ''How do I know if I am a victim? cppasia.com.sg; June 2014,accessed February5,2017*

[37] *Ibid 243*

[38] *See section 2.2.2 on worldwide statistics*

[39] *Heith Copes, Anastasia Brown, Identity Theft; May 23, 2012;oxfordbibliographies.com;Accessed December 26,2016.*

[40] *Identity Theft Resource Center website.idtheftcenter.org, Accessed December 26,2016*

[41] *Identity Theft Resource Center, What does financial identity theft involve?idtheftcenter.org. Accessed December 26, 2016.*

[42] *MasterCard, Identity Theft and ATM-related Fraud Top Payments Security Concerns: MasterCard Research,mastercard.com; Singapore ,August 20 2015?*

[43] *Ibid*

[44] *Identity Theft Statistics show increasing global issue,armourcard.com; Accessed December 26,2016*

[45] *Short video available to illustrate*

no matter how savvy or cautious someone is with the actual and real possibility to have been ‘‘elbow to elbow’’ with the fraudster at the time of committing and not notice that you are being ripped off. It actually gives cold sweats. Somehow the level of insecurity generated by ID thieves is significant.

The Development of online fraud has led government agencies to encourage victims to file a complaint for both national and international scams[46] as part of national awareness programmes around the world. This allows governments agencies and law enforcement to have real time information about fraud types and schemes and consequently formulate appropriate measures and more stringent remedies against fraud perpetrators.

IV. CASE STUDY

A. Identity Theft using credit card: Case of Amar and Neha Punjani-Singh[47]

i. Credit Card Forgery:

Amar Sing and his wife were members of 5 organized gangs specialized in forged credit card and identity theft based in Queens County and ties to Europe, Asia, Africa and the Middle East. According to the court document reports they netted more than $13 million in losses within 16months following a scam that involved the use of skimming devices to steal credit card information from customers of retail stores, and illegal identification gathering websites. Teams of ‘‘shoppers’’ were sent out on shopping expeditions in New York, Florida, Massachusetts, Los Angeles and other areas of US to purchase merchandise for personal use and re-sold over the internet. The police Commissioner said ‘‘these were not holdups at gunpoint, but the impact on victims was the same…They were robbed. The potential of victimization is great, especially as the use of credits cards and their vulnerability to identity theft have grown along with internet’’. Amor and Neha Punjani-Singh were found guilty of manufacturing counterfeit credit card and identity theft charges along with criminal enterprises and enterprise Corruption under New York State’s Organized Crime Control Act.

ii. Legal Analysis

This case is a talking example of the environment in electronic transactions; how personal information land into the hands of fraudsters and the use they make of it afterward. Beside internal fraud with international elements is more and more E-transactions fraud trend. Associations of Fraudsters rob for personal use or for resale purpose. Identity theft is a threat to national and international households and economies.

iii. Identity Theft Using Virtual Currency

a. Case of Western Express International, Inc.[48]

b. Transnational ID Theft Using Virtual Currency as a tool for money concealment

The investigation conducted US Secret Service and the Manhattan (New York County) District Attorney’s Office conducted jointly the investigation of the Western Express, a multinational, resulted in convictions or guilty pleas for fraud associated with other unlawful acts of 16 of its members for their role in a global identity theft/cyber fraud including reshipping schemes. The New York Corporation based in Manhattan operated as a virtual currency exchanger and unregistered money transmitter to coordinate and facilitate the internet payment methods and to launder the group’s proceeds. Members of the group located in Ukraine, also throughout Eastern Europe and the United States managed web sites devoted to trafficking in stolen credit card and personal identifying information and used false identities, anonymous instant messenger accounts, anonymous email accounts, and anonymous

---

[46] FTC, ‘‘Filling a Complaint’’ available at https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/filing-complaint,accessed February 14, 2017. See also ‘‘Consumer Action: How to Complain’’ September26, 2012, P.4. Further See Colleen Tressler, ‘‘Reporting International Scams’’ Consumer Information may be consulted at https://www.consumer.ftc.gov/blog/reporting-international-scams.October 13, 2015.

[47] District Attorney Queens County, Release 166-2011,Friday October 7,2011;PDF

[48] Financial Action Task Force (FATF), Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014, P.14.

virtual currency accounts to conceal the existence and purpose of the enterprise. 100 000 stolen credit card numbers and other personal identification information were sold through the Internet, mostly in e-Gold and Web Money. The buyers used the stolen identities to forge credit cards and purchase merchandise for their personal use. The fraudulent activities generated about USD 5 million in credit card fraud proceeds.

This case highlights two figures. Fraudsters are wont to use not only one method but two or three associated at once; that way they cause a larger impact on the victims. Second the joint action between two different stakeholders within the same country. Such cooperation is needed not only at internal level but at international level as well for E-transactions frauds are more and more exported out of national authorities' reach.

V. IDENTITY THEFT LEGAL REMEDIES

Identity theft costs consumers and businesses billions of dollars in loss. Consequently, these losses have triggered legislative and regulatory responses. However, whilst some articles and reports refer to ID theft as a crime, others qualify it as a fraud.[49] While Canada and United States consider it a serious crime, some European countries classify it as a fraud.[50]Other countries such as India and Philippines refer to ID theft as a cybercrime.[51] The lack of uniformity is a godsend for fraudsters. Indeed, different qualifications of Identity theft lead to different definitions and diverse legislation as well. This circumstance hinders the true efficiency of laws and fraudsters can easily get away.

A. Existing Legal Remedies

In OECD countries, ID theft is subject to different legal characterizations, leading to different enforcement schemes. While the US and Canada refer to it as serious crime, some EU member states classify it as fraud.[52] In France, a person convicted of identity theft is fined up to 75,000 euros.[53] In United States, the Congress enhanced the identity theft laws by passing the Identity Theft Enforcement and Restitution Act of 2008.[54] The Act authorized restitution to identity theft victims for their time spent recovering from the harm caused by the actual or intended identity theft. Likewise, the Identity Theft Task Force was established in May 2006 by Executive Order 13402 to conduct fraud investigations and track fraudsters committing ID theft and other related unlawful acts[55] Under Hong Kong Laws, the Theft Ordinance in its chapter 210, Section 16A states.[56] In India, under the Information

---

[49] *My TermPapers.com ''Identity Theft in Asia'', July 2016, P1-22*

[50] *OECD Observer, Online Identity Theft 268, available at http://oecdobserver.org/news/archivestory.php/aid/2662/Online_identity_theft/html; June 2008 ; Accessed December 2016.*

[51] *Kuril Bora, India High On The List Of Countries Impacted By Ransomware, Identity Theft And Phishing Attacks: Report,ibtimes.com, October 23,2013.Accessed February 3,2017.*

[52] *OECD Observer, Online identity theft,N0 268,available at http://oecdobserver.org/news/archivestory.php/aid/2662/Online_identity_theft.html;June 2008,Accessed December 2016.For example in US, the Identity Theft Assumption Deterrence Act criminalizes identity theft at a federal level(See Kristin Finale in Identity Theft: Trends and Issues, January 16,2014;Congressional Research Service Report; in addition to making ID theft a crime, this act provides penalties for individuals who either committed or attempted to commit identity theft and provides for forfeiture of property used or intended to be used in the fraud.P.4*

[53] *Olivier Iteanu, Usurpation d'identité: la loi ou la technique pour se protéger? journaldunet.com; accessed in December 26,2016*

[54] *Title II of P.L.110-326 A VERIFIER*

[55] *Executive order 13402, ''Strengthening Federal Efforts To Protect Against Identity Theft,'' 71 Federal Register 93,may 15,2006*

[56] *(1) If any person by any deceit(whether or not the deceit is the sole or main inducement) and with intent to defraud induces another person to commit an act or make an omission, which results either*

Technology Act 2000 Chapter IX Section 66C, the ID theft perpetrator undergoes imprisonment[57] and to fines which may extend to rupees one lakh. Philippines which ranks eighth in the numbers of users of Facebook and other social networking sites has been known as source of various identity theft problems.[58]

This phenomena led to the creation of Bill 52: cybercrime Prevention Act of 2002. Section 2 of the Bill imposes[59] to violators a fine upwards of Php200, 000 but not exceeding one million or depending on the damage caused.

The observation is that the measures are different from one country to another.

Technology may also evolve as helpful means to combat identity theft.[60] But As ever when it comes to building trust, multi-stakeholder co-operation is a vital part of the answer.

ID theft had also raised some initiatives at international level. 2007, the UN Office on Drugs and Crime (UNODC), developed a set of recommendations on ID-related crimes[61] calling on authorities, the private sector and civil society to join efforts to fight ID theft. Following the lead, the 2008 OECD[62] Ministerial Conference on the Future of the Internet Economy recognized the benefits of co-operation.

The fact that ID theft is sometimes qualify as a crime, a fraud, an aggravated fraud, a serious crime or even a cybercrime does not help to harmonize the legal measures. This circumstance will be difficult to manage in cross-order fraud cases that especially necessitate outside borders investigation; and the reality is that happens a lot in E-transactions fraud.

B. Proposals for new range of remedies

The long run of e-transactions fraud can considerably be reduced by a range of more stringent remedies. It is critical to build the capacity of legislation; So that they could deal with E-transactions fraud given the role that fraud perpetrators play in disturbing the ongoing smoothness of online commercial interactions. In participating in E-transactions, consumers shall be willing to file a complaint and report the fraudulent act. Without actual denunciation of fraudsters by customers, law enforcement would be incapable to link cases that have a factual connection and more importantly keep a record of these complaints in order to have a clean estimation of each type of E-transactions fraud and means of committing. The key to enhance the effectiveness of anti-E-transactions fraud is not only the augmentation of tracking operation to break fraudsters cover, although these have proven successful in many ways. Rather, the key to enhancing current capabilities is extending civil remedies. Many states changing their consumer protection laws are an illustration of the fact that the past laws or existing laws are no

---

(a) in benefit to any person other than the second mentioned person; or(b) in prejudice or a substantial risk of prejudice to any person other than the first mentioned person, the first-mentioned person commits the offense of fraud and is liable on conviction upon indictment to imprisonment for 14 years.

[57] ''Punishment for identity theft whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other 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 which may extend to rupees one lakh' '(is a unit in the Indian numbering system equal to one hundred thousand; it is written as 1,00,000. For example in India 150,000 rupees becomes 1,5 lakh rupees).

[58] List of Facebook Users By Country wise Top Ranking 2016,tonystable.com,Accessed December26,2016

[59] Philippines through the Bill 52 recognizes the importance of communication and multimedia for the development, exploitation and dissemination of information.

[60] OECD Observer No 268, June 2008,oecdobserver.org;Accessed December 26,2016

[61]UNDOC Recommendations on ID-related crimes UN, 2007,

[62] Brigitte Aooca, Online Identity Theft, OECD Directorate for Science, Technology and Industry. Available at http://oecdobserver.org/news/archivestory.php/aid/2662/Online_identity_theft.html.Visited, February 14, 2017.

more appropriate for e-commerce environment. All these laws carry stringent rules at the expense of sellers and revised the compensation regime. Thus, in China the remedies under the now amended consumer law of 1994 was10.000 Yuan.

Under the new consumer law, he who is guilty of fraud should pay 3times the loss amount and the statutory amount is 500,000 Yuan which is 10 times under the consumer rights protection amended law. For the time being, the remedy is substantial. However what about in 20 or 40 years when technology is more advanced and fraudsters most genius than ever? As such shall be considered:

1- Life time civil remedies without imprisonment and with layers.
With no jail time, the fraudsters will have to work and pay to compensate the victims of his fraudulent act. Nevertheless, the proposal goes with layers starting by 1(one) year remedy and walk its way through according to the loss of the victim. Each country shall revise and see the way that suits the best. Not only at national level, but this proposal shall serve as basis for the adoption of an international instrument that will lay out more specifics about the underlying civil remedy proposal.

2- Adopting international exclusively civil remedies instrument on e-transactions fraud
E –transactions fraud has ceased to be only a domestic problem. With the development of technology, fraudsters have expanded their activities from national to international level. And yet, to date so far not a single instrument on E-transactions fraud exist that gather intelligence and policyholders around the world. It has been individual initiatives like OECD, nothing collective like usual that could help reduce considerably the scourge. On contrary, inversely almost each region of the world has enacted a cybercrime instrument.[63] According to UNODC, globally 82 countries have signed and/or ratified a binding cybercrime instrument.[64] The reality is reversed when it comes to adopt E-transactions fraud international instrument. We believe an international instrument on E-transactions fraud especially for remedies shall benefit countries and serve higher purposes in terms of:

Harmonization of e-transactions fraud definitions and remedies:

- To avoid ‘‘safe harbors’’ for fraudsters-In the field of E-transactions fraud with international elements, the main advantage of harmonization lies in the prevention of fraud safe havens for perpetrators. Online fraud materialized in Identity theft, e-retail and auction fraud, Telecommunications fraud to name a few is a global problem and this makes all countries important in one of several ways. International cooperation between States is important on the basis that E-transactions know no boundaries. Indeed, Electronic transactions fraud may offer direct risk for use of safe harbors. Thus, if the remedies for harmful acts stem from fraud involving E-transactions are more extensive for example in State Y but not in State Z, a perpetrator of fraud in State Z can be free to target victims in State Y via the internet. In such cases, State Z cannot effectively and efficiency on its own protect against effects from such transnational activities.

- To express seriousness. The reason beneath State adopting more cybercrime international instruments[65] versus zero on E-transactions fraud is that fraud occurring in E-transactions is overlooked by States because most of the financial lost are small amounts. However considered all together, fraudulent activities perpetrated at a large scale engage a large number of victims as well so plenty of money. The extension of civil remedies will bring a particular notice on the matter and reverse things. More the remedies are stringent more they will be indicative of the level of seriousness of E-transactions fraud which does not discriminate, be it at domestic or international level.

3-Another principle shall be considered in the international instrument which is that of supplemented remedy.
The principle of supplemented remedy shall be applied on the basis of the initial proposal to respond to the difficulty generated by various definitions and laws applicable to e-transactions fraud from one country to another. It shall bring a solution to cross-border e- transactions fraud cases. The supplemented remedy would consist for example for a fraudster caught in a transnational fraud activity to compensate the victim twice, first under the law of the country where the fraudulent act occurred (may or may not be the fraudster’s country) and second under the law of the country where the injured victim lives (that may or may not also be the country of the fraudster).Of

[63]*The Commonwealth of independent States, The council of Europe, Intergovernmental African organizations,,, the league of Arab States and the United Nations. According to UNODC, globally 82 countries have signed and/or ratifies a binding cybercrime instrument (Comprehensive study on Cybercrime-February 2013).What we can’t tell when it comes to E-transactions Fraud knowing that there are both internet production.*
[64] *Ibid*
[65] *Where some E-transactions fraud are generally referred to as cybercrimes*

course the principle shall not apply if the perpetrator and the victim live both in the same country. In that case, the country's usual regime regarding civil remedies apply. The supplemented remedy shall serve as deterrence for fraudsters in order to protect citizens of both countries. Furthermore, for the purposes of harmonization of fraud definitions and remedies, the important point is that the dual remedy does not require that the underlying activity be addressed by the same type of legal provision knowing that countries have different background and ground reality. Thus if State B uses a crime offence for particular conduct for online auction fraud, whilst State A uses a general offence, both B and A will be able to engage in cooperation, provided that the essential constituent elements of the fraudulent act are comparable under the laws of both states. Indeed, a general observation of legislation regarding some E-transactions fraud[66] shows a diversity of qualification. For instance identity fraud is referred to either as a crime or a cybercrime or an aggravated fraud[67] all according to the country.

VI. CONCLUSION

Identity theft is a threat to e-transaction. Besides the fact that the tactics used by fraudsters to generally commit identity theft are evolving, it is nowadays associated with one or two other e-transactions fraud. This circumstance comes as a real challenge to law enforcement. Besides the lack of uniformity in the qualification of e-transactions fraud is a godsend for fraudsters. Indeed, different qualifications of Identity theft lead to different definitions which in turn call different legislation as well. This circumstance hinders the true efficiency of laws and fraudsters already hidden behind anonymity that online environment offers can easily get away. For starters, States shall try to find an identical definition of identity theft at international level and do the same for the civil remedies or system of compensation. Internet users are relying on the law to protect their interests and guide their choices for a better participation in the single market extolled by the majority of States to enhance their economy. Where there is a will there is a way. A recommendation related to the creation of an international instrument dedicated essentially to civil remedies for fraud occurring in e-transactions would be a good way to start dealing with this problem.

[66] *See generally Chapter III on Case study of E-transactions fraud and legal remedies*
[67] *In India and Philippines Identity Theft is a Cybercrime. US Court distinguish between simple identity theft and aggravated identity theft.*