دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

| | |
|---|---|
| العنوان: | Cyber Crime and Money Laundring |
| المؤلف الرئيسي: | alhammad, Omar abdullah |
| موقع: | Wollongong |
| الصفحات: | 1 - 38 |
| رقم MD: | 752513 |
| نوع المحتوى: | رسائل جامعية |
| الدرجة العلمية: | رسالة ماجستير |
| الجامعة: | Wollongong University |
| الكلية: | Faculty of Law |
| الدولة: | أستراليا |
| قواعد المعلومات: | Dissertations |
| مواضيع: | الجرائم، الجرائم الإلكترونية، غسل الأموال |
| رابط: | http://search.mandumah.com/Record/752513 |

© 2016 دار المنظومة. جميع الحقوق محفوظة.
هذه المادة متاحة بناء على الإتفاق الموقع مع أصحاب حقوق النشر، علما أن جميع حقوق النشر محفوظة. يمكنك تحميل أو طباعة هذه المادة للاستخدام الشخصي فقط، ويمنع النسخ أو التحويل أو النشر عبر أي وسيلة (مثل مواقع الانترنت أو البريد الالكتروني) دون تصريح خطي من أصحاب حقوق النشر أو دار المنظومة.

# Cyber crime and money laundring


# Omar abdullah alhammad

# Master of transantional crime preventioon

# University of wollongong


# For the library of saudi cullture mission in australia

# Introduction

## 1.1 Background of the Study

Ecommerce has necessitated increased transference of funds, information and data from one person to another through emails and website technology, from one account to another through the electronic payment systems especially through the internet as well as through social networking sites. Today, people are buying goods and services around the world through the internet, without the need to travel to shops. The upsurge of the internet technology and networking will continue to drive these trends upwards, as more and more people continue to absorb it in their culture. Internet dealings have largely been admired because of the speed with which they can deliver products and services as compared to traditional methods. They have increased the reduction of costs of data and information sharing and transfer, they have reduced errors associated with information as well as led to delivery of messages in a more stylistic comfortable means.

Thus, payment methods, and generally, methods for exchange of data and information between persons and organizations through the internet are being practiced more and more. They are therefore becoming very prone to attacks from people who are targeting these transfer lines, so as to gain unauthorized access of data for evil motives. Data being transmitted across two or more people can be tapped and used for other reasons such as forging for money withdrawals from online accounts, access of people's accounts as well for other purposes. There are many people who are making payments online and fraudsters are using this as a channel to steal money through compromising data and access points. Continued usage of online payment systems will mean that more hackers and fraudsters will be interested in their deals than before, hence the need to study the crime and role in money

laundering. Financial institutions can now move funds through Electronic Funds Transfer (EFT) System across the globe with the click of mouse. Besides legitimate beneficiaries- banks, airlines, media, universities, non-financial businesses- of information and communication technologies (ICT) and the internet, criminals take advantage of ICT and the internet to commit various types of cyber crimes, such as, hacking; spamming; spoofing; cyber terrorism; cyber forgery; plastic card (debit/credit and stored value cards) and cyber fraud. Cyber fraud is one of the effective tools in the hands of cyber criminals which generates huge amount of illegal money without being detected by law enforcement agencies because cyber crime is the crime with anonymity. Furthermore, cyber crime can be committed in various jurisdictions of world simultaneously therefore it involves transnational jurisdiction, which poses great challenges for law enforcement agencies to prevent, detect and investigate such crimes. Transnational nature of cyber crime supports criminals to commit crime without being detected by law enforcement agencies; therefore, world is witnessing increased number of cyber crimes. As discussed above, cyber crime can generate huge amount of illegal money. Such money is of course illegal and requires laundering to avoid detection by law enforcement agencies. Therefore, cybercriminals use cyber technology to hide the true origin of their criminal proceeds to look like clean money. This process is known as money laundering.[1]

**1.2 Problem Statement**

Globalisation has increased the movements of goods and services across the world, which has increased economic interdependence resulting in profound benefits and opportunities.[2] The benefits and opportunities include quick and easy travel of people across the globe; quick

[1] Rajev Saxena, 'Cyberlaundering: The Next Step for Money Launderers?'(1998) 10 *Saint Thomas Law Review* 685, 685.

[2] Santha Vaithilingam and Mahendhiran Nair, 'Mapping Global Money Laundering Trends: Lesson from the Pace Setters' (2009) 23 *Research in International Business and Finance* 18, 18.

movement of funds from one part of the world to another with the help of electronic funds transfer (EFT) system- FedWire, Society for worldwide Interbank Financial telecommunication (SWIFT) code, Clearing House Inter Payment system (CHIPS)-[3], plastic cards and Internet banking- cyberpayment systems.[4] The technology and innovation are the drivers of widening of globalization,[5] which is not only being used by legitimate users but also but illegitimate users. The illegitimate users of technology are using internet and technology for generating illicit proceeds as well as for laundering illegitimate proceeds, which pose great challenge for law enforcement agencies to prevent, detect, investigate and prosecute such technology-based crimes as it involve transnational jurisdiction. Therefore, there is a need to understand how technology and internet is used by cyber criminals for generating illegal proceeds and by cyber-launderers for laundering illicit proceeds.

**1.3 Purpose of Research**

The main purpose of this research proposal is to twofold. First purpose is to understand how criminals are generating illegal proceeds by the commission of cyber crime. Second, how cyber-launderers are exploiting technology and internet for laundering ill gotten money by using plastic cards- Debit Card, credit Card and Stored value Card. The research will help law enforcement agencies to formulate effective policies and procedures for detecting, preventing and investigating such crimes.

**1.2 Aims and Objectives of the Study**

The main purpose of this research proposal is to twofold. First purpose is to understand how criminals are generating illegal proceeds by the commission of cyber crime.

[3] Gregory Calpakis et al, *Study Guide for the CAMS Certification Examination* (4th ed, 2007), 29.

[4] James R Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering : a Handbook for Law Enforcement Officers, Auditors, and Financial Investigators* (1999) Accessed: UoW Database at 02 September 2010.

[5] Santha Vaithilingam and Mahendhiran Nair, 'Mapping Global Money Laundering Trends: Lesson from the Pace Setters' (2009) 23 *Research in International Business and Finance* 18, 18.

Second, how cyber-launderers are exploiting technology and internet for laundering ill gotten money by using plastic cards- Debit Card, credit Card and Stored value Card. The research will help law enforcement agencies to formulate effective policies and procedures for detecting, preventing and investigating such crimes.

**1.4 Hypothesis**

This study will seek to test the following hypothesis as relates to money laundering through cyber crime.

i. Money laundering cases are increasing and mostly connected to online business dealings (ecommerce) and connection between companies and their customers.
ii. Little has been done on the international law perspective in defining and covering cyber crime. This would be required to ensure that the issues relating to the modern types of crimes are solved amicably and responsibly without contradictions.
iii. A large amount cyber crime behaviour can be dealt with through observance of the basic rules set regarding handling of communications over the internet or that cyber crime has flourished amidst carelessness and little concern, or ignorance among the users of related services.
iv. The complexity of the computer and electronic systems as well as security issues (and relatively newness of computer dealings) has had its own contribution in the advancement of cyber crime involved in money laundering.

**1.5 Significance of the Study**

Money laundering has been practiced for quit long time now. It is live on many countries and on the international scene, and companies have suffered from the practices, loosing billions of money. Cyber crime has diverse problems, and therefore, its solution will have more advantages to the online trader than just loosing money. Just to focus on a few, cyber crime

has had an impact of compromising privacy and confidentiality of online dealers, through unauthorized access to their private data and confidential accounts. Cyber crime is thus a breach of individual rights to privacy and confidential information as captured in many legal frameworks of many countries. Information regarding the execution of cyber crime will be expected to lead the way in helping solve this problem. Loosing money through cyber criminals has been experienced by companies and hence it is necessary that these type of crime be combated using a comprehensive legal framework on the international scene, so as to save many organizations from collapse. Such a study would provide adequate information regarding how cyber crime related to money laundering takes place, and how it can be avoided. Usually, it would be expected that knowledge on the most current trends of cyber crime involving laundering of money through debit cards would help in chatting the way forward against the vice. There are two ways through which cyber crime may be combated; formulating an international legal framework that captures the whole issue regarding cyber crime, and secondly, countering the crime through best technology suited for this purpose. It is therefore necessary that there be studies regarding the trends of occurrence and impacts of cyber crimes.

There has been much attempt to ensure that cyber crime has been combated through basic mechanisms. Usually, providers of electronic systems have tried to ensure security through a number of mechanisms. It can already be established that cyber crime has flourished amidst little knowledge and lack of awareness of the complex issues surrounding cyber crime among the users. Cyber criminals almost certainly will be successful where issues of security are overlooked as far as payments are concerned. Thus, the information regarding the occurrence of cyber crime would be beneficial so as to help the general user on the best way to secure

their communications. In addition, organizations would be expected to observe even the basic rules regarding communications in an attempt to keep away the cyber criminals.

**2.0 Literature review**

A number of scholars have separately researched the issues of generating illegal proceeds by committing cyber crimes and cyber laundering- laundering of illegal proceeds by the use of cyber technology. *Peter Grabosky* refers that cyber space has abandoned physical borders and cyber criminals can easily commit crimes across the borders; therefore, modern crimes are becoming transnational in nature. He further adds that cyber crime is used in both conventional crimes such as pornography, piracy fraud and forgery and in modern crimes for example, hacking; phishing. *Grabosky* claims that huge illegal money can be generated from the commission of cyber frauds, which can further laundered through cyber technology. He refers to the case of Russian hacker, Vladmir Levin, who compromised Citibank's electronic funds transfer system and transferred heavy amount from the accounts of corporate customers of Citibank into the accounts of his accomplices in various jurisdictions- Israel, United States, the Netherlands, Finland and Germany.[6] *Adam Salifu* adds that financial institutions are one of the victims of cyber crimes, for example, plastic card frauds; which cause huge financial losses to financial institutions. According to author, cyber crime is of transnational nature to that extent that the offenders and victims are available in different jurisdictions, therefore, it becomes challenging job for law enforcement agencies.[7]

*Richards* claims that "cyber payment system" or "cyberbanking" has taken over traditional currency system: paper notes, coin, cashier checks or any other financial instruments. In modern period money has become "financial value" which can easily be transferred from one

[6] Peter Grabosky, 'the Global Dimensions of Cyber crime' (2004) 6 *Global Crime* 146, 146, 48.
[7] Adam Salifu, 'the Impact of Internet Crime on Development' (2008) 15 *Journal of Financial Crime* 432, 437-8.

place to another place through plastic cards and Internet banking by cyberpayment systems.[8] *Saxena* is of point of view that it is very easy for money launderers to hide illegal proceeds in financial system and subsequently transfer proceeds by using technology based products, for example, plastic cars (debit/visa/stored value cards) and electronic funds transfer system. He evidences that argues that criminals can instantaneously transfer huge amounts of funds in a very short time by using technology.[9] *Jaarsveld* refers to some other aspects of technology which are helpful for criminals to launder money. He states that Internet has made easy for everyone to make quick transactions from remote areas by maintaining the anonymity of the users. He further adds that "capacity" is one of the effective tools in the hands of users of online transactions. One can make huge transactions across the borders which also poses a great challenge for law enforcement agencies to make trail of these transactions. It is also difficult for financial institutions to keep record of internet / online transactions.[10]

*Weaver*'s research refers that "cyberlaundering" is one of the favourable tool in the hands of criminals not only to launder proceeds but also generate illegal proceeds through online casinos and other gambling websites. *Weaver* argues that physical cash has been replaced by "e-money" in the shape of "stored value cards (SVC)".He adds that e-money can be stored on SVC in the form of bits, therefore, huge amount can easily be stored on such cards, which is very easy to carry as compared to physical cash. E-money is not only easy to carry but it is also easy to keep anonymity because the SVCs can be used from any part of the globe. The authors further add that e-money can be loaded on SVCs as well as on hard disks of the

[8] James R Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering : a Handbook for Law Enforcement Officers, Auditors, and Financial Investigators* (1999) 30-1.
[9] Ibid, 688.
[10] Izelde Van Jaarsveld, 'Following the money Across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'(2004) 16 *South African Mercantile Law Journal* 685, 691.

computers. Therefore, it will be difficult for customs and other law enforcement and border agencies to detect illegal smuggling of huge amount of cash. Moreover, the users of e-money can withdraw cash from Automated Teller Machines (ATMs); therefore, it gives a great opportunity for money launderers to launder illegal proceeds through e-money.[11] *Welling* and *Rickman* state that use of electronic payment system is increasing rapidly; which gives various facilities to its users. He refers to the Mondex card frequently used in United Kingdom (UK), which provides facility to its users to transfer cash on Mondex card from their internet bank account. Moreover, the users of Mondex cards can also transfer amount from one Mondex card to another without obtaining help from intermediary. Furthermore, the users of Mondex can make payment on the Mondex terminals as well as can withdraw money from Mondex enabled ATMs. This transfer of funds either from internet ban account or from Mondex card to Mondex card and making payment at terminals or withdrawing money through ATMs provides opportunity to the criminals to launder huge funds in different places by maintaining anonymity and remote locations,[12] which will enable them to avoid detecting from law enforcement agencies.

*Schopper* refers to another aspect of technology which is used for laundering proceeds of crime: Internet gambling. He says that over the period of time number of Internet gambling websites has increased. The author adds that the users of internet gambling make payment through plastic cards (Debit / Credit cards) or through electronic funds transfer system for online gambling. Once the payment is made by the users, he/she can gamble on the online

[11] Stephen Jeffery Weaver, 'Modern day Money Laundering: Does The Solution Exist in An Expansive System of Monitoring and Record Keeping Regulations?' (2005) 24 *Annual review of banking and Financial Law* 443, 450.
[12] Sarah N Welling and Andy G Rickman, 'Cyberlaundering: the Risks, the Responses' (1998) 50 *Florida Law Review* 295, 306.

gambling websites and after some bets, these online gamblers request websites to return money, which apparently is a gambling winning and receives sanitized check / pay order from these online websites.[13] *Mussington,Wilson* and *Molander* refer to another mode of internet gambling- "electronic sports bookmaking". In this version of Internet gambling, the players bet on the results of the matches of various sports for example, baseball; football; horse racing and other games. This type of Internet gambling involves transfer of funds from users to Internet gambling sites and vice versa. Transfer of funds to and from these Internet gambling website include "cyberpayment" system, for example; plastic cards transfers and online / Internet banking transfers.[14]

Moreover, Internet banking is one of the technology-based areas through which money can be laundered. According *Andrew Zerzan*, Internet banking provides facility to customers to operate their accounts and avail their banking services without being physically visiting the banks, for example, deposit of cheques, transfer of funds, lending services, and plastic card operations/use.[15] Williamson claims that the Internet banking involves less service costs as compared to conventional banking, therefore, number of users of internet banking is increasing. Moreover, the Internet banking is facing challenges of cyber attacks, for example, phishing; data theft; and other cyber attacks, which can pose serious threat to the financial institutions.[16] *Neil Munro* adds that the products offered by internet banking are at nascent stage but its pace is fast. He claims that "remote access" and "speed of movement" are

[13] Mark D Schopper, 'Internet Gambling, Electronic Cash & Money Laundering: The Unintended Consequences of a Monetary Control Scheme' (2002) 5 *Chapman Law Review* 303, 305.

[14] David A Mussington, Peter A Wilson and Roger C Mplander, 'Exploring Money Laundering Vulnerabilities through emerging Cyberspace Technologies: A Caribbean-Based Exercise' (1998) *Critical technology Institute RAND* 26-7.

[15] Andrew Zerzan, 'New technologies, New Risks? Innovation and Countering the Financing of Terrorism'(2010) Word Bank paper No. 174

[16] Gregory D Williamson, 'Enhanced Authentication in Online Banking' (200) 6 *Journal of Economic Crime Management* 1, 2.

characteristics of Internet banking which are being exploited by launderers to launder their illicit proceeds and pose great challenges for law enforcement agencies because money launderers can quickly transfer their proceeds to offshore financial centres (OFCs). A drug dealer, human trafficker or any other criminal can deposit their funds in any unregulated financial institutions and can quickly move their funds to different jurisdictions, which will be difficult for law enforcement agencies to track the funds transfer.[17]

*John Madinger* adds that cash is becoming obsolete. Funds are now electronically transferred not only by banks but also by stock brokers; money service business- Western Union; credit card companies- Visa Card, MasterCard; governments through cyberpayment systems like FedWire, Society for worldwide Interbank Financial telecommunication (SWIFT) code, Clearing House Inter Payment system (CHIPS). *Madinger* claims that every year approximately 250,000 electronic transfers of illicit money are carried out around the globe.[18] *Gregory Calpakis et al* claim that money launderers can transfer their proceeds between different jurisdiction and bank accounts with the help of electronic funds transfer (EFT) within seconds. The quick transfer from one country to another country, from one bank to another bank, from one account to another make it difficult for law enforcement agencies to identify the origin and trail of proceeds. He claims that launderers can easily hide illegitimate proceeds within millions of dollars legal transfers and it will be hard for law enforcement agencies to segregate illegitimate and legitimate transfers.[19]

Informal value transfer (IVT) system is one of the methods of laundering criminal proceeds, which involves traditional as well as technology based transfers from one jurisdiction to

[17] Neil Munro, 'Internet-Based Financial Services: A New Laundry?' (2001) *Journal of Financial Crime* 134, 145-6.
[18] John Madinger, *Money Laundering: A Guide for Criminal Investigation* (2nd ed, 2006) 225, 40..
[19] Gregory Calpakis et al, *Study Guide for the CAMS Certification Examination* (4th ed, 2007) 15, 29.

another jurisdiction. *Shirma Keene* adds that the other name for IVT is alternative remittance system (ARS) and some where it is named as *hawala*. She claims that in modern period funds transfer from one jurisdiction to another jurisdiction through *hawala* system involves financial institutions; therefore, modern *hawala* system also involves technology-based fund transfers.[20] *El-Qorchi* says that *hawala* operators are called as *hawaldars*, who transfers money from one country to another country. He adds that *hawala* system siphon off funds from developing countries; therefore, it causes "capital flight" from developing countries. Moreover, most of *hawala* transactions are cash based; therefore, there are less chances of having paper trail of such transactions. The author claims that *hawala* transactions are also used to control exchange control as the transactions are cash based.[21]

*Passass* claims that penetration in *hawala* system and investigations is very difficult by law enforcement agencies particularly after September 11, 2001 attacks on USA the *hawala* operators have posed serious challenges for law enforcement agencies. *Passass* further claims that there are serious implications of *hawala* operations in any jurisdictions because it helps criminals to hide their illicit proceeds easily without being detected by law enforcement agencies. Moreover, *hawala* transactions can also be commingled with licit transactions and it become challenging for law enforcement agencies to unearth illicit transactions hidden in licit transactions. *Passass* says that modern time *hawala* transactions are conducted with the help of Internet, "correspondent" accounts and "payable though accounts", which adds another layer of difficulty for law enforcement agencies to prevent, detect and investigate *hawala* transactions. According to *Passass*, the record keeping and customer identification in

[20] Shima Keene, '*Hawala* and Related Informal Value Transfer Systems- An Assessment in the Context of Organized Crime and Terrorist Finance: Is there Cause for Concern?' (2007) 20 *Security Journal* 185, 185, 8.
[21] Mohammed El-Qorchi, 'Hawala: Based on Trust, Subject to Abuse' (2004) *Economic Perspectives* 22, 24.

*hawala* is minimal; therefore, it is favourite option for money launderers to transfer illegal proceeds from one jurisdiction to another jurisdiction.[22] *Trehan* says that *hawala* is an "underground banking system", which is hidden and operated through front legitimate companies; jewellery shop; exchange houses; and "unregulated" financial centres. The authors further adds that details of money senders is transmitted at destination places in encrypted form and in codes in order to hand over the money to its accurate recipient. The authors refers to another dark side of *hawala* operations that it is used to use illegal money in real estate.[23]

[22] Nikos Passass, 'Law Enforcement Challenges in Hawala-Related Investigations'(2004) 12 *Journal of Financial Crime* 112, 112-3.

[23] Jyoti Trehan, 'Underground and Parallel Banking System' (2002) 10 *Journal of Financial Crime* 76, 76, 80.

**2.1 Cyber Crime and Banking**

A number of scholars have separately researched the issues of generating illegal proceeds by committing cyber crimes and cyber laundering- laundering of illegal proceeds by the use of cyber technology. *Peter Grabosky* refers that cyber space has abandoned physical borders and cyber criminals can easily commit crimes across the borders; therefore, modern crimes are becoming transnational in nature. He further adds that cyber crime is used in both conventional crimes such as pornography, piracy fraud and forgery and in modern crimes for example, hacking; phishing. *Grabosky* claims that huge illegal money can be generated from the commission of cyber frauds, which can further laundered through cyber technology. He refers to the case of Russian hacker, Vladmir Levin, who compromised Citibank's electronic funds transfer system and transferred heavy amount from the accounts of corporate customers of Citibank into the accounts of his accomplices in various jurisdictions- Israel, United States, the Netherlands, Finland and Germany.[24] *Adam Salifu* adds that financial institutions are one of the victims of cyber crimes, for example, plastic card frauds; which cause huge financial losses to financial institutions. According to author, cyber crime is of transnational nature to that extent that the offenders and victims are available in different jurisdictions, therefore, it becomes challenging job for law enforcement agencies.[25]

*Richards* claims that "cyber payment system" or "cyberbanking" has taken over traditional currency system: paper notes, coin, cashier checks or any other financial instruments. In modern period money has become "financial value" which can easily be transferred from one

[24] Peter Grabosky, 'the Global Dimensions of Cyber crime' (2004) 6 *Global Crime* 146, 146, 48.

[25] Adam Salifu, 'the Impact of Internet Crime on Development' (2008) 15 *Journal of Financial Crime* 432, 437-8.

place to another place through plastic cards and Internet banking by cyberpayment systems.[26] *Saxena* is of point of view that it is very easy for money launderers to hide illegal proceeds in financial system and subsequently transfer proceeds by using technology based products, for example, plastic cars (debit/visa/stored value cards) and electronic funds transfer system. He evidences that argues that criminals can instantaneously transfer huge amounts of funds in a very short time by using technology.[27] *Jaarsveld* refers to some other aspects of technology which are helpful for criminals to launder money. He states that Internet has made easy for everyone to make quick transactions from remote areas by maintaining the anonymity of the users. He further adds that "capacity" is one of the effective tools in the hands of users of online transactions. One can make huge transactions across the borders which also poses a great challenge for law enforcement agencies to make trail of these transactions. It is also difficult for financial institutions to keep record of internet / online transactions.[28]

*Weaver*'s research refers that "cyberlaundering" is one of the favourable tool in the hands of criminals not only to launder proceeds but also generate illegal proceeds through online casinos and other gambling websites. *Weaver* argues that physical cash has been replaced by "e-money" in the shape of "stored value cards (SVC)".He adds that e-money can be stored on SVC in the form of bits, therefore, huge amount can easily be stored on such cards, which is very easy to carry as compared to physical cash. E-money is not only easy to carry but it is also easy to keep anonymity because the SVCs can be used from any part of the globe. The authors further add that e-money can be loaded on SVCs as well as on hard disks of the computers. Therefore, it will be difficult for customs and other law enforcement and border

[26] James R Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering : a Handbook for Law Enforcement Officers, Auditors, and Financial Investigators* (1999) 30-1.
[27] Ibid, 688.
[28] Izelde Van Jaarsveld, 'Following the money Across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet'(2004) 16 *South African Mercantile Law Journal* 685, 691.

agencies to detect illegal smuggling of huge amount of cash. Moreover, the users of e-money can withdraw cash from Automated Teller Machines (ATMs); therefore, it gives a great opportunity for money launderers to launder illegal proceeds through e-money.[29] *Welling* and *Rickman* state that use of electronic payment system is increasing rapidly; which gives various facilities to its users. He refers to the Mondex card frequently used in United Kingdom (UK), which provides facility to its users to transfer cash on Mondex card from their internet bank account. Moreover, the users of Mondex cards can also transfer amount from one Mondex card to another without obtaining help from intermediary. Furthermore, the users of Mondex can make payment on the Mondex terminals as well as can withdraw money from Mondex enabled ATMs. This transfer of funds either from internet ban account or from Mondex card to Mondex card and making payment at terminals or withdrawing money through ATMs provides opportunity to the criminals to launder huge funds in different places by maintaining anonymity and remote locations,[30] which will enable them to avoid detecting from law enforcement agencies.

*Schopper* refers to another aspect of technology which is used for laundering proceeds of crime: Internet gambling. He says that over the period of time number of Internet gambling websites has increased. The author adds that the users of internet gambling make payment through plastic cards (Debit / Credit cards) or through electronic funds transfer system for online gambling. Once the payment is made by the users, he/she can gamble on the online gambling websites and after some bets, these online gamblers request websites to return money, which apparently is a gambling winning and receives sanitized check / pay order

[29] Stephen Jeffery Weaver, 'Modern day Money Laundering: Does The Solution Exist in An Expansive System of Monitoring and Record Keeping Regulations?' (2005) 24 *Annual review of banking and Financial Law* 443, 450.

[30] Sarah N Welling and Andy G Rickman, 'Cyberlaundering: the Risks, the Responses' (1998) 50 *Florida Law Review* 295, 306.

from these online websites.[31] *Mussington,Wilson* and *Molander* refer to another mode of internet gambling- "electronic sports bookmaking". In this version of Internet gambling, the players bet on the results of the matches of various sports for example, baseball; football; horse racing and other games. This type of Internet gambling involves transfer of funds from users to Internet gambling sites and vice versa. Transfer of funds to and from these Internet gambling website include "cyberpayment" system, for example; plastic cards transfers and online / Internet banking transfers.[32]

Moreover, Internet banking is one of the technology-based areas through which money can be laundered. According *Andrew Zerzan*, Internet banking provides facility to customers to operate their accounts and avail their banking services without being physically visiting the banks, for example, deposit of cheques, transfer of funds, lending services, and plastic card operations/use.[33] Williamson claims that the Internet banking involves less service costs as compared to conventional banking, therefore, number of users of internet banking is increasing. Moreover, the Internet banking is facing challenges of cyber attacks, for example, phishing; data theft; and other cyber attacks, which can pose serious threat to the financial institutions.[34] *Neil Munro* adds that the products offered by internet banking are at nascent stage but its pace is fast. He claims that "remote access" and "speed of movement" are characteristics of Internet banking which are being exploited by launderers to launder their illicit proceeds and pose great challenges for law enforcement agencies because money

[31] Mark D Schopper, 'Internet Gambling, Electronic Cash & Money Laundering: The Unintended Consequences of a Monetary Control Scheme' (2002) 5 *Chapman Law Review* 303, 305.

[32] David A Mussington, Peter A Wilson and Roger C Mplander, 'Exploring Money Laundering Vulnerabilities through emerging Cyberspace Technologies: A Caribbean-Based Exercise' (1998) *Critical technology Institute RAND* 26-7.

[33] Andrew Zerzan, 'New technologies, New Risks? Innovation and Countering the Financing of Terrorism'(2010) Word Bank paper No. 174

[34] Gregory D Williamson, 'Enhanced Authentication in Online Banking' (200) 6 *Journal of Economic Crime Management* 1, 2.

launderers can quickly transfer their proceeds to offshore financial centres (OFCs). A drug dealer, human trafficker or any other criminal can deposit their funds in any unregulated financial institutions and can quickly move their funds to different jurisdictions, which will be difficult for law enforcement agencies to track the funds transfer.[35]

*John Madinger* adds that cash is becoming obsolete. Funds are now electronically transferred not only by banks but also by stock brokers; money service business- Western Union; credit card companies- Visa Card, MasterCard; governments through cyberpayment systems like FedWire, Society for worldwide Interbank Financial telecommunication (SWIFT) code, Clearing House Inter Payment system (CHIPS). *Madinger* claims that every year approximately 250,000 electronic transfers of illicit money are carried out around the globe.[36] *Gregory Calpakis et al* claim that money launderers can transfer their proceeds between different jurisdiction and bank accounts with the help of electronic funds transfer (EFT) within seconds. The quick transfer from one country to another country, from one bank to another bank, from one account to another make it difficult for law enforcement agencies to identify the origin and trail of proceeds. He claims that launderers can easily hide illegitimate proceeds within millions of dollars legal transfers and it will be hard for law enforcement agencies to segregate illegitimate and legitimate transfers.[37]

Informal value transfer (IVT) system is one of the methods of laundering criminal proceeds, which involves traditional as well as technology based transfers from one jurisdiction to another jurisdiction. *Shirma Keene* adds that the other name for IVT is alternative remittance

[35] Neil Munro, 'Internet-Based Financial Services: A New Laundry?' (2001) *Journal of Financial Crime* 134, 145-6.
[36] John Madinger, *Money Laundering: A Guide for Criminal Investigation* (2nd ed, 2006) 225, 40..
[37] Gregory Calpakis et al, *Study Guide for the CAMS Certification Examination* (4th ed, 2007) 15, 29.

system (ARS) and some where it is named as *hawala*. She claims that in modern period funds transfer from one jurisdiction to another jurisdiction through *hawala* system involves financial institutions; therefore, modern *hawala* system also involves technology-based fund transfers.[38] *El-Qorchi* says that *hawala* operators are called as *hawaldars*, who transfers money from one country to another country. He adds that *hawala* system siphon off funds from developing countries; therefore, it causes "capital flight" from developing countries. Moreover, most of *hawala* transactions are cash based; therefore, there are less chances of having paper trail of such transactions. The author claims that *hawala* transactions are also used to control exchange control as the transactions are cash based.[39]

*Passass* claims that penetration in *hawala* system and investigations is very difficult by law enforcement agencies particularly after September 11, 2001 attacks on USA the *hawala* operators have posed serious challenges for law enforcement agencies. *Passass* further claims that there are serious implications of *hawala* operations in any jurisdictions because it helps criminals to hide their illicit proceeds easily without being detected by law enforcement agencies. Moreover, *hawala* transactions can also be commingled with licit transactions and it become challenging for law enforcement agencies to unearth illicit transactions hidden in licit transactions. *Passass* says that modern time *hawala* transactions are conducted with the help of Internet, "correspondent" accounts and "payable though accounts", which adds another layer of difficulty for law enforcement agencies to prevent, detect and investigate *hawala* transactions. According to *Passass*, the record keeping and customer identification in *hawala* is minimal; therefore, it is favourite option for money launderers to transfer illegal

[38] Shima Keene, '*Hawala* and Related Informal Value Transfer Systems- An Assessment in the Context of Organized Crime and Terrorist Finance: Is there Cause for Concern?' (2007) 20 *Security Journal* 185, 185, 8.
[39] Mohammed El-Qorchi, 'Hawala: Based on Trust, Subject to Abuse' (2004) *Economic Perspectives* 22, 24.

proceeds from one jurisdiction to another jurisdiction.[40] *Trehan* says that *hawala* is an "underground banking system", which is hidden and operated through front legitimate companies; jewellery shop; exchange houses; and "unregulated" financial centres. The authors further adds that details of money senders is transmitted at destination places in encrypted form and in codes in order to hand over the money to its accurate recipient. The authors refers to another dark side of *hawala* operations that it is used to use illegal money in real estate.[41]

## 3.0 Participation of Money Laundering with Plastic Cards

### 3.1. Online ID theft and Practice

A group of people from the "United States Postal service", the "Department to of homeland security", Department of Justice" as well as the "Department of Treasury" were involved in interagency working and came up with a report, "Money Laundering Threat Assessment (MLTA)" and which seeks to exploit "13 channels through which money launderers may take advantage of the U.S. financial system"[42]. The report, titled "Stored Value Cards" also identifies vulnerabilities regarding the use of prepaid cards. Also addressed in this category was the type of cards which are issued outside the United States but can be utilized in United States. Again, the area of interest included those cards issued in the United States and is applicable outside the country.

[40] Nikos Passass, 'Law Enforcement Challenges in Hawala-Related Investigations'(2004) 12 *Journal of Financial Crime* 112, 112-3.

[41] Jyoti Trehan, 'Underground and Parallel Banking System' (2002) 10 *Journal of Financial Crime* 76, 76, 80.

[42] Sienkiewicz, Stanley, 'Prepaid Cards: Vulnerable to Money Laundering?' (2007). Retrieved 12 October 2010 from http://www.compliancealert.org/pdfs/The_plastic_money_laundry.pdf

This report, which exposed 13 ways through which the U.S financial system has been taken advantage of by the money laundering business, is of the argument that the "easy transportability and the relative ease of moving and potentially accessing monetary value anonymously" makes the cards prone to money laundering. Those at the greater risk of money laundering are those cards which "do not require customer identification" or that "do not include rigorous monitoring of suspicious activity" according to this report.

Money laundering and its potential vulnerability has also been discussed by the National Drug Intelligence Center (NDIC). Noting that prepaid card provided "an ideal money laundering instrument to anonymously move monies associated with all types of illicit activity" the report notes that it is required that "due diligence procedures" regarding "prepaid stored value cards" should be endorsed by financial institutions since "open and semi-open system prepaid stored value cards are used in a manner that approximates a traditional checking account" according to Sienkiewicz :2[43].

The Financial Action Task Force also released a report regarding prepaid cards in 2006, capturing the cards which "allow for electronic cros-border fund transfers that might also facilitate money laundering" as cited in Sienkiewicz: 2[44]. Some of the environments viewed as most prone to money laundering were featured as programs which incorporated "offshore card issuers and access to cash at ATMs as environments" as posited in Sienkiewicz: 3[45].

[43] See [24]

[44] See [24]
[45] See [24]

The private sector has been geared towards understanding the vulnerability associated with credit cards in an attempt to develop strategies aimed at mitigating the problem[46]. Sienkiewicz has differentiated the vulnerability of prepaid cards to money laundering business from "more traditional payment card fraud" (p. 3). The author has featured how the response of government and the payment industry in an attempt to curb the problem "while still supporting innovation" (p. 3)[47].

### 3.2 Plastic Cards

Plastic cards come in various types depending on their uses. They can be used for gaining or controlling access to places that are restricted-called the Access Control Card, loyalty card where an organization or a charity benefits from co-branding partnership (called an affinity card), barcode cards and blank cards, charge card where credit can be provided to the holder automatically for a given period, cheque guarantee card which allows holders (members of a building society) to pay cheques to people or for the purpose of cashing out cheques, chip card, city card, combi card among others.

### 3.3 Online ID theft

Credit and debit cards contain information that sellers are willing to ask for so as to charge people's accounts once they commit to pay online. Thus, provision of this data can pave way for crime if it lands to bad hands. Sometimes, companies may be genuine, but put this information in such a way that it will finally be accessed and used illegally. Again, there are sites that ask for credit card information yet they are not encrypted or secure and this poses a risk for the user because there information may land on bad hands and be used illegally. There is need to ensure that such information is provided to companies that keep it secure.

[46] See [24]
[47] See [24]

Those offers on credit card which have been pre-approved are also not the best options because the information may be left back with the company and can be used illegally. Unused credit cards also need to be destroyed.

**3.4 Technology of Online Theft and Other Compromises**

Technology is high regarding money laundering as far as plastic cards are concerned. Whether you are using a debit card or a prepaid card or any other type, of most important is your personal information. Once it is compromised, the type of the card remains irrelevant. There are many ways through which attackers are using to compromise security of the cards. These include phishing. In 2003, the amount lost (from US banks and credit card issuers) as a result of phishing was $1.2 billion according to Emigh[48]. This is where attackers may try to gain access of the personal information through use of fraudulent software (malware attacks), tricks to the user to render the information, as well as diverting the user to a fraudulent server through use of altered host names.

Sometimes, fraudsters may use traditional methods to trick users of plastic cards to render personal information, for example through pretense or misrepresentation (they may for example pretend to be the bank and call the customer). This is termed as social engineering and grouped under the category of phishing. Another way of social engineering is where, through use of emails, customers may be tricked and directed to counterfeit websites (presented as particular company names) and divulge personal data information such as giving card numbers and passwords. In addition, technology has allowed the planting of crimeware onto users' PC so that the personal identification information such as the plastic card numbers are practically stolen "directly, often suing Trojan keylogger spyware as

[48] Emigh, A. (2005). Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures. Retrieved 9 September 2010 from http://www.antiphishing.org/Phishing-dhs-report.pdf

posited in McAfee[49]. Once they get these numbers, they apply them for criminal activities, either withdraw money or manufacture fake cards.

Customers of prepaid card networks have also been tricked to render information through pharming, where the users are directed to "fraudulent sites or proxy servers, typically through DNS hijacking or poisoning" so as to have their details for cards obtained.

### 3.4 Prone Areas for Plastic Money Laundering

#### 3.4.1 Introduction

"Consumer electronic payments" have given rise to the prepaid cards as a relatively new development. Consumers have responded to "gift cards" well, through the sale activity of the retail merchants. Pre-funding characteristic has been incorporated through invention in the credit card arena. It has been possible to link the prepaid cards with other card networks such as the mastercards and Visas thus their application is far beyond that of gift cards. They have been utilized as alternatives to "traditional paper-based solutions" including "governant assistance programs", "cross-border remittances" as well as "payroll payments" as cited in Sienkiewicz[50]. It has been expressed that these cards are very useful as far as serving the "undeserved" societies and those "unbanked" societies.

However, these cards have been targeted for crime through the same features that have given them competitive advantages over other forms of payment. These cards have been the target for money launderers according to study by Sienkiewicz[51].

[49] McAfee. (2006). Phishing and Pharming: Understanding phishing and Pharming. Retrieved 10 October 2010 from http://www.mcafee.com/us/local_content/white_papers/wp_phishing_pharming.pdf

[50] See [24]

[51] See [24]