Humanity & Social Sciences Journal 7 (1): 18-22, 2012
ISSN 1818-4960

DOI: 10.5829/idosi.hssj.2012.7.1.25213

Crime of the Millennium: Cyber Crime

[1]Zakir Gul and [2]Ramazan Terkesli

[1]Turkish National Police Academy, Intelligence Studies Research Center, Ankara, Turkey
[2]Turkish National Police, Information Technology Department, Ankara, Turkey

Abstract: Credit card fraud, as the fastest growing crime of the new millennium, puts a great burden on the economy affecting both customers and financial institutions. It not only costs money, but also a great amount of time to restore the harm done. Biometric verification systems and smart cards are among the alternative solutions. On the other hand, the intelligence community should update itself in terms of technology and awareness programs.

Key words: Cyber Crime, Identity Theft, Credit Card Fraud, Biometrics, Smart Cards, Ingelligence Gap

INTRODUCTION

The 21st century appeared to be a century of possibilities and opportunities with the introduction of the advanced information technologies for both legal and illegal activities. The life style and the possibilities have created a variety of opportunities that facilitate and sometimes even encourage credit card fraud. Plastic payment systems as one of these innovations of the century have provided a great deal of comfort as well as risks to the customers in terms of the technology used. With just a few touches, one can do online banking, buy or sell something, or even earn money.

As mentioned, there are risks involved in using such a highly advanced technology. One can have his/her name on the most wanted persons list of the police even without his/her knowledge. A hacker from the other side of the world can use someone else's computer to gain valuable personal information or just to use your computer as a 'zombie' to launch attacks on other computer systems. But, at the end of the day, it will be someone who will be in danger because of the traces that his/her computer left behind in all the way that the hacker passed through [1]. In this respect, identity theft and credit card fraud as the most prevalent type of identity theft, appears to be the crime of the new millennium. In addition, credit card fraud is the fastest growing crime in the United States and costs billions of dollars to the customers, to the businesses and to the credit card companies, banks and other financial institutions.

A Cyber Crime: Identity Theft and Credit Card Fraud: As the technology has progressed worldwide, the complexity of the crimes has also grown enormously in the last century. Especially in last two decades, the computer and cutting-edge internet technologies have made it possible for criminals to commit the most sophisticated crimes ever. Earlier, the crimes were very basic in nature and criminals did not need complicated techniques. People, or lets say police in specific, might detect criminals and crimes in the past by even searching with bare eyes or at least people could identify them in the stores or maybe in the streets at night whilst they tried to steal something.

However today, there are certain types of crimes that victims can only be aware of after years and it is nearly

Corresponding Author: Ramazan Terkesli, Turkish National Police, Information Technology Department, Ankara, Turkey. Tel: +9031246242606, E-mail: rterkesli@egm.gov.tr.

impossible to track down all of those criminals, who can steal money even without the knowledge of the owner. Furthermore, they can steal people's identities and can impersonate others in the cyber space, opening new accounts or shopping with an endless greed. When people realize that they have been a target of such crimes like credit card fraud or identity theft, it is, most of the times, too late. It is very difficult and sometimes impossible to restore their credit history and clean 'their' notorious files and sometimes to prove that they were not the ones who committed a series of crimes.

Fraud and theft offenses constitute the biggest proportion of the cyber crimes since the main motivation of the criminals is personal and economic profit. When the "victim's identity is stolen, the primary criminal use of this information is credit card fraud" [2]. It is predicted that "organized crime groups will become more involved in identity theft related crime such as credit card fraud and that these crimes will become increasingly transnational [2]. The identity theft "is neither consistently defined nor consistently used describes criminal acts where the perpetrator fraudulently obtains and uses another person's identity" [3]. Since e-commerce has been more and more widespread day by day, these types of cyber offenses are positing the most serious threat. The most widespread forms of cyber fraud are online auction fraud and investment fraud. On the other hand, cyberspace is a convenient place for cyber criminals to commit theft by threat or extortion [4]. Another kind of cyber fraud that can be easily committed over the internet is credit card fraud [5].

Today, in the 21st century, it is difficult to differentiate and distinguish between certain crimes like most of the frauds and identity theft crimes. This is because, even criminal needs to provide 'real' information to a bank to open a new account, or he/she will need some very personal information like social security number and mother's maiden name. Thus, committing a credit card fraud, or any other financial crime, for most of the times, involves some kind of id theft as well. Therefore, identity theft and credit card fraud are linked and intertwined.

According to the US Postal Inspection Service, "ID theft is America's fastest growing crime. Last year alone, more than 9.9 million Americans were victims of identity theft, a crime that cost them roughly $5 billion" [6] and according to the Federal Trade Commission's Identity Theft Survey, the total number of victims in the last five years mounted up to 27 million people in the US [7].

College students are shown as the most potentially vulnerable mass to identity theft, due to their non-established and clean credit histories and whom identity particulars are easily accessible from school records through various ways, facilitated especially by the advancement of information technologies [8]. LoPucki [9] argues that the Congress' first attempt to respond the problem (i.e. the enactment of the Identity Theft and Assumption Deterrence Act of 1998) has had little effect in combating identity theft due to the way, current credit-reporting system operates. Basically, in the case of identity theft, the identity thief obtains money, goods, credit, or services, charges them to the real owner of that identity and then disappears. To commit identity theft, it is enough for an imposter to obtain the victim's name, social security number, birth date or mother's maiden name, because it is widely accepted that knowing these personal information is enough to prove of being that person [9].

And at the end, Id theft victims face several problems like a bad credit history, sometimes being arrested for crimes that certainly the person did not commit himself and of course he/she even does not know what consequences might arise after getting their identity stolen.

Some Evidence: Hoar (2001, US DOJ Website) argues that on May 1, 1998, the General Accounting Office (GAO) released a briefing report where it stated that "methods used to obtain identity information ranged from basic street theft to sophisticated, organized crime schemes involving the use of computerized databases or the bribing of employees with access to personal information on customer or personnel records". Furthermore, "The Secret Service stated that actual

[1]Hoar [10] also quotes: "Trans Union Corporation, one of the three major national credit bureaus, stated that two-thirds of its consumer inquiries to its fraud victim department involved identity fraud. Such inquiries had increased from an average of less than 3,000 a month in 1992 to over 43,000 a month in 1997. VISA U.S.A., Inc. and MasterCard International, Inc. both stated that overall fraud losses from their member banks were in the hundreds of millions of dollars annually. MasterCard stated that dollar losses relating to identity fraud represented about 96 percent of its member banks' overall fraud losses of $407 million in 1997."

losses to individuals and financial institutions which the Secret Service had tracked involving identity fraud totaled $442 million in fiscal year 1995, $450 million in fiscal year 1996 and $745 million in fiscal year 1997."[1]

May and Headley [11] argue that the total cost of identity theft to the economy in 2004 both to the customers and financial institutions exceeds $ 5 billion in the United States. Credit card fraud consists 42% of the total identity theft crimes which is $ 2.1 billion. Moreover, "The problem is growing at an alarming rate" (p.3) and the target of this crime are 170 million card holders in the United States (Ibid., p. 51).

Katayama [12] argues that "If 8 million card accounts were affected and all those cards were canceled with new cards issued in their place, it would cost the credit card companies an estimated $200 million, according to credit card experts" (CNN Website) And worse than that is that "Often, when credit card accounts are hacked, account numbers and other information obtained may be sold to others who, in turn, may use that information to make unauthorized purchases." It is shown on the National Center for Policy Analysis Website [13] that "it typically takes victims 14 months to discover the identity theft --and often another two years to resolve it" and "The biggest loss is usually in time away from work while dealing with the problem."

What Can Be Done?

Alternative 1 – Increasing Financial Literacy and Education: According to a recent survey, 22% of banking customers said that while they had received a notice of privacy rights they had not read it [11]. So, financial literacy education is a must for such a number of financially illiterate people who are more likely to fall victim of fraud today or another day. It is best understood when we consider the existence of 170 million card holders, approximately %90 of adults, in the United States [11]. So, educating people about protecting their personal information and supporting victims of identity theft is important.

The government should help educate consumers about the practical steps that they and often only they can take to prevent identity theft. For example, consumers should closely monitor their accounts for unusual or unexplained transaction or for missing statements or replacement credit cards. Early knowledge is one of the best ways of restricting the thief's use of stolen personal information. Of course, early knowledge is only useful if the consumer reports the fact to creditors, credit bureaus and law enforcement authorities.

Alternative 2 – Biometrics[2]: Fingerprint Identification: O'Sullivan [14] states that "The beauty of a biometric trait is that it is as unique as the individual from whom it was created. Unlike a password or PIN, a biometric trait cannot be lost, stolen, or recreated". Although the use of biometric identification systems requires lots of financial resources, they are the most effective way of identification. For instance, ThumbPod has a false accept rate of 0.01 percent and a false reject rate of less than 1 percent [15]. However, this alternative does not involve identification, but verification because it needs a great amount of data traffic to make identification [16]. Therefore, cardholders could also go to one of their banks and give their fingerprints for identification purposes and these fingerprints to be stored in a national database for verification. Once the customer wants to use his/her card, he/she will also be required to put his/her thumb for fingerprint verification so that the system will know the cardholder and the person trying to use the card are actually the same person. The scanner will transfer the fingerprint into digits and transfer them to the national data center for matching the fingerprint codes.

Alternative 3 –Smart Cards: A Smart Card is "a standard credit card-sized plastic intelligent token within which a microchip has been embedded within its body and which makes it 'smart'"[3]. Smart cards[4] have been in use in Europe for

[2]It is also argued that "Fingers, hands, eyes, face, voice, all are in use and could relegate PIN-based security to history" [14]

[3]Retrieved from http://www.ewh.ieee.org/r10/bombay/news5/SmartCards.htm on April 10, 2008

[4]"The chip and PIN system is designed to guard against credit card fraud by requiring customers to tap in a four digit number - rather than signing a payment slip - when paying for their goods." [19]

many years. Leyden [17] states that "A similar domestic PIN-based system in France has seen an 80 per cent reduction in fraud since its introduction ten years ago".

Alternative 4 – Filling Intelligence Gaps: If the number of id theft, particularly credit card fraud, is high and still continues to be high, then it means these criminals cannot be closely watched and followed. Surveillance techniques should be updated and improved in terms of technology and human source development. The state officials have to be as confident and knowledgeable in this virtual world as they are in the actual one. The logic of tracking a crime/criminal never changes. The criminal leaves some traces somehow, somewhere, sometime one way or another. The application of the intelligence/surveillance techniques should be applied/used in the cyber world as soon as possible in order to get rid of the gaps and hence prevent the increase of such crimes.

CONCLUSION

In conclusion, the foundation of criminal justice system is to keep order and secure justice in the society. Safety is one of the basic needs of people according to Maslow's [18] pyramid of hierarchical needs and crime prevention, in this respect, emerges as a necessity for development of a healthy and safe society. Therefore, the state has to be one step ahead the criminals in terms of the use of technology or the control/surveillance of the technology in order to prevent unlawful actions in cyberspace. As the uncontrolled power is not (a true and just) power, similarly, the uncontrolled technology is not (a helpful and good) technology for citizens. Without safety, which is one of their basic needs, the citizens will not feel like they are living in a free and happy World. As Thompson [8] finalized his writing "The government, public and private institutions, businesses, organizations and individuals must all give the definition and protection of identity the highest attention, in the interest of both individual and national security" (p. 65).

REFERENCES

1. Burden, Kit and Creole Palmer, 2003. "Internet crime: Cyber Crime - A new breed of criminal?" Computer Law and Security Report, 19(3): 222-227.
2. Finklea, K.M., 2012. Identity Theft: Trends and Issues. Congressional Research Service Report for Congress, http://www.crs.gov on December 10, 2012.
3. Javelin Strategy and Research, 2008. Identity Fraud Survey Consumer Report, available at: http://itsecurity.und.edu/2008%20Identity%20Fraud%20Survey%20Report.pdf/ (last visited: Dec. 2012). For further information on other surveys see Chawki/Abdel Wahab, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006 – available at: http://www.lex-electronica.org/docs/articles_54.pdf/ (last visited: Dec. 2012).
4. Goodman, M.D. and S.W. Brenner, 2002. "The emerging consensus on criminal conduct in cyberspace". International Journal of Law and Information Technology, 10(2): 139-223.
5. Davis, E.S., 2003. A world wide problem on the World Wide Web: "International responses to transnational identity theft via the internet". Washington University Journal of Law and Policy, 12: 201-227.
6. United States Postal Inspection Service, 2008. "ID theft is America's fastest growing crime". Retrieved from http://www.usps.com/postalinspectors/idthft_ncpw.htm on April 1, 2008.
7. Synovate, 2003. "Federal Trade Commission – Identity Theft Survey Report" prepared in September 2003. Retrieved from http://www.ftc.gov/os/2003/09/synovatereport.pdf on March 25, 2008.
8. Thompson, J.F., 2002. "Identity, privacy and information technology". Educause Review, 37(6): 64.
9. LoPucki, L.M., 2001. "Human identification theory and the identity theft problem". Texas Law Review, 80(1): 89.

10. Hoar, S.B., 2001. Identity theft: The crime of the new millennium. In U. S. Department of Justice (Ed.) (Vol. 49, 2): United States Attorneys' USA Bulletin. Derived from http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm on March 28, 2008.
11. May, David A. and James E. Headley, 2004. Identity Theft. New York: Peter Lang.
12. Katayama, F., 2003. "Hacker hits up to 8M credit cards" Retrieved from CNN Web Site: http://money.cnn.com/2003/02/18/technology/creditcards on April 3, 2008.
13. National Center for Policy Analysis, Retrieved from http://www.ncpa.org/pi/crime/pd051101c.html on April 4, 2008.
14. O'Sullivan, O., 2005 "Biometrics comes to life" Retrieved from http://www.banking.com/aba/cover_0197.htm on March 25, 2008.
15. Lee, H., 2004. "New security device a handy way to stop credit card fraud." Retrieved from Daily Bruin Web Site: http://www.dailybruin.ucla.edu/news/2004/apr/08/new-security-device-a-handy-wa/ on March 27, 2008.
16. Schuddekopf, P., 2003. "ID Theft and Credit Card Fraud Can Be Significantly Reduced with Two New Technologies Developed by Hypercom" Retrieved from http://www.secureidnews.com/news/2003/01/01/id-theft-and-credit-card-fraud-can-be-significantly-reduced-with-two-new-technologies-developed-by-hypercom/ on April 1, 2008.
17. Leyden, J., 2003. "Joe Public blames banks for credit card fraud" Retrieved from Help Net Security Web Site: http://www.net-security.org/news.php?id=2964 on April 2, 2008.
18. Maslow, A.H., 1943. "A Theory of Human Motivation" Psychological Review, 50: 370-96.
19. Leyden, J., 2003. "Smart credit on UK cards: Will it cut fraud?" Retrieved from The Register Website http://www.theregister.co.uk/2003/04/11/smart_credit_on_uk_cards/ on April 11, 2008.
00. Fraud Watch International, 2008. "Identity Theft" derived from http://www.fraudwatchinternational.com/identity-theft/ on April 1, 2008.
00. US General Accounting Office, 1998. "Identity Fraud" derived from official website http://www.gao.gov/archive/1998/gg98100b.pdf on March 30, 2008.