Journal of Forensic Sciences & Criminal Investigation

Juniper Publishers key to the Researchers

Case Report
Volume 1 Issue 4 - January 2017

J Forensic Sci & Criminal Inves

Digital Data Stealing from ATM using Data Skimmers: Challenge to the Forensic Examiner

Mukesh Sharma[1]* and Shailendra Jha[2]

[1]*Department of Physics, Regional Forensic Science Laboratory, India*

[2]*Department of Physics, State Forensic Science Laboratory, India*

Submission: December 10, 2016; **Published:** January 19, 2017

***Corresponding author:** Mukesh Sharma, In-charge, Assistant Director, Department of Physics, Regional FSL, Bharatpur, India, Tel: +91-9460986307; Email: mksphy@gmail.com

Abstract

Automated Teller Machines (ATMs) are secured money dispenser machines easily operated now available at nearest corner of our ally. Secured cards are used to operate these machines. By the passage of time they are not as secured, as presumed. Now these are highly venerable to the fraud. An Important component of the machine is card reader that initiates the machine for further action. Criminals are high-tech these days and cleverly stealing information and data written on the credit-cards which is generally presumed as secured by common non- techno-savvy user. Apart from concealed camera picture of the PIN number of the user, Peeping through shoulder of the user, which are easily detectable way used by the criminals a highly reliable and easy to use gadget called Digital skimmers are in use. Skimming, a form of high-tech financial fraud, is on the rise worldwide. However, ATM card fraud, that crime which most people associate with ID theft, decreased as a percentage of all ID theft complaints for the sixth year in a row, ATM frauds in the India even and across the world. In present paper authors have discussed use of various kind of skimmer used by the criminals and the tricks to theft the ID of individuals.

Keywords: ATM; PIN; Skimmers; Credit-cards; Mini 400 SMR

Abbreviations: ATMs: Automated Teller Machines; POS: Point-of-Sale; PINs: Personal Identification Numbers; VPD: Vancouver Police Department

Introduction

ATM skimmers are high-tech bank robbers known as while paper crime. Instead of using a gun and a note, skimmers use fake card readers and hidden cameras to steal a customer's information to get to that customer's money and take it. Skimming has become big business. ATM scams are becoming more frequent, but ATM kiosks are not the only machines targeted. Using a debit card at the store, malls and Petrol pumps can be risky and created scam victims. Not only can they steal our account information, but our PIN also. Hackers are now targeting bank ATMs. Identity theft is only the start of a chain of events that ultimately cost victims money. It is not the theft of identity alone that concerns people; rather, it is the financial losses that identity theft enables. Skimmers are data-reading electronics to copy the magnetic stripe information from your credit card or debit card. In the early days of skimming scams, criminals used to fix a card-skimming device into the card insertion slot. The skimmer could then steal account information stored on the magnetic strip of the swipe card [1-3]. Skimming, a form of high-tech financial fraud, is on the rise worldwide. It relies on sophisticated data-reading electronics to copy the magnetic stripe information from your credit card or debit card. In Figure 1, the statistical data of all over the world showing the number of victims as card fraud are increasing year by year. The criminals who create these "skimming" devices have a high level of technical knowledge.

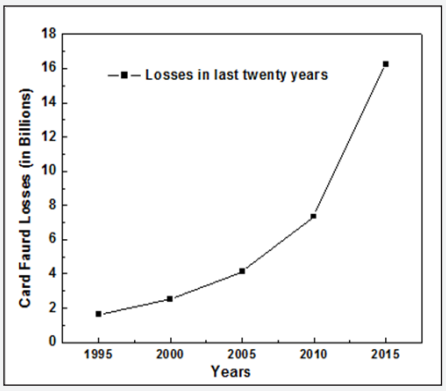


Figure 1: Steady increase in the number of victims of card fraud losses over 20 years.

Furthermore, they must install these devices in point-of-sale (POS) terminals or automated teller machines (ATMs) to gain access to victim card data and personal identification numbers (PINs).Untapped investigative opportunity exists in the seizure of modified POS terminals and ATM overlays. This column examines these opportunities and describes what one Canadian agency, the Vancouver Police Department (VPD), has done to identify these technological criminals and prevent identity theft [4-5]. Figure 2, showing the primary components ID theft. A criminal generally slip an electronic magnetic strip reader over the existing card slot at an ATM. When a card is tagged/scream in, the skimming device reads it first, and then the actual card reader at the point of transaction, rest of the process go in the same way as real without your even realizing it. Petrol pumps are most vulnerable places today are largely automated and often unattended, giving criminals plenty of opportunity to embed skimming devices in late at night.

Figure 2: Primary components of identity theft.

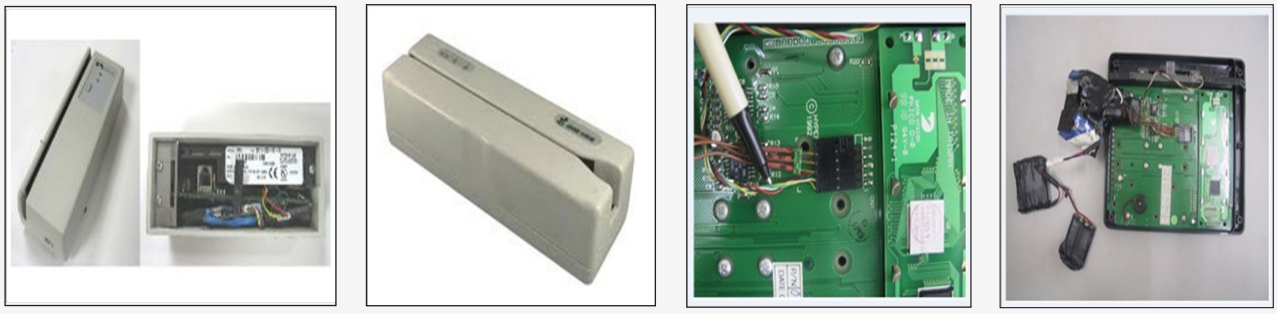
Our case study

In a case registered by the Special Investigation Group in Rajasthan, Lap-Top computers, CPU, Blank magnetic Cards, Fake credit-Cards, CDs, Pen-drive, Card read -writer, Chargers, Cables and small size small Skimmers like items were recovered during raid from suspected five persons. The suspects stated that they were preparing membership cards of their company, but they were storing any data/information stolen from the cards of the genuine credit-card holders onto the magnetic strip of the card, so that they can clone the identity and misuse the information of the card holders for illegal means [6].

Result and Discussion

A collective approach was opted for examination of these articles. The exhibits were examined in the laboratory. Encase software was used for examination of the hard disc of the Lap-Top, CPU and pen-drive. Read- write software was used to read data stored onto the magnetic card. Deleted information was retrieved from the Hard-Disc of the Lap-Top and CPU. There were many deleted files with the details of the credit-cards of Indian and foreigners. Some files were having names of foreigners stored with the name of Japanese names, Germen names. Scanned images of the foreigner's and Indian passports were also retrieved from the hard disc.

Product identification and name of the electronic gadgets were scratched to hide the identity of the product. The electronic gadgets were identified as MSR 206 Magnetic card read-writers and Tysso, Mini 400 is a very small magnetic-card reader. Mini 400 is a very small magnetic swipe card reader with the software controlled password security for users. The device is so small that it can be hidden in the cuff of the sleeve of the house coat or apron generally put-on by the waiters in the hotels (Figures 3A & 3B). This gadget can be fastening in the wrist of a person with the help of an elastic wrist band. A waiter can wear the wrist band with skimmer and before giving to the bill clerk he can easily swipe the credit-card in the Mini 400 series magnetic card reader. The gadget has a battery back-up it can retain the data. Some of the plastic cards were golden in colour and no data was stored on the magnetic strip, some were white and some were blank with monogram of master card [7].



3(a) 3(b)

3(A) **3(B)**

Figure 3a: Small size Skimmer.

Figure 3b: MSR Read-Writer.

Figure 3A: Skimmer devices and its internal components.

Figure 3B: Mini connectors (tapping onto tape head reader) and battery back-up.

How to cite this article: Mukesh S, Shailendra J. Digital Data Stealing from ATM using Data Skimmers: Challenge to the Forensic Examiner. J Forensic Sci & Criminal Inves. 2017; 1(4): 555567.

Stealing PIN

One of the most common high-tech ways to steal PINs is with tiny cameras mounted within a fish-eye mirror and with an electronic mesh overlaid on the keyboard. PINs may be four digits long. When you key in your PIN, software at the ATM automatically converts it into a one-way algorithm called "Hash". Then, if someone captures the data steam, they'll see only the resulting hash value, not the original four or six digits. By itself, a "Hashed Pin" is a useless string of numbers but free software is available to convert these Hashed value to a digit and the job is over. This way a duplicate credit - card was generated in the case as discussed earlier. Data written on these card was copied from the file found stored in the CPU and in the pen-drive. Names were picked from the scanned passport. Individual details were picked through skimmer together was sufficient to create a duplicate credit-card [8]. In Figure 4, the retrieve file of American names opened in notepad. In Figure 5, the credit card information skimmed by the skimmer, stored in the fine, containing lot of information in it.

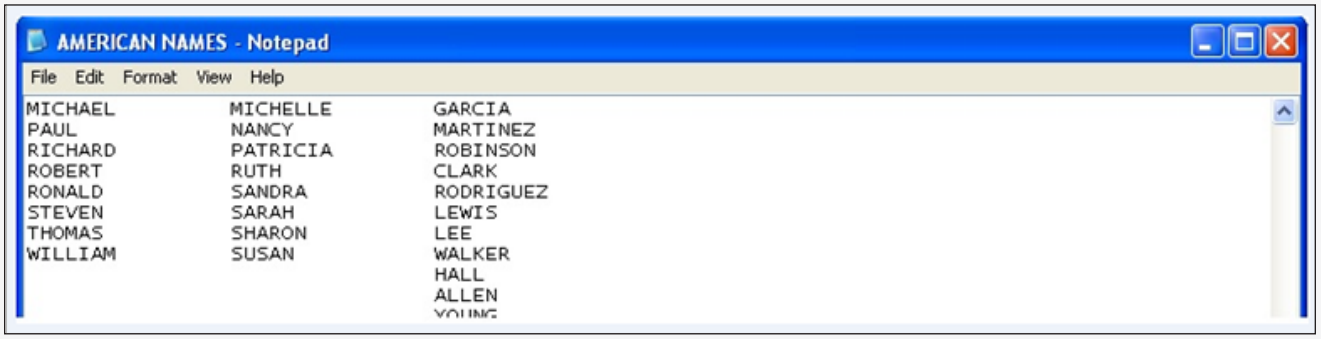


Figure 4: File showing name and surnames of foreigners.

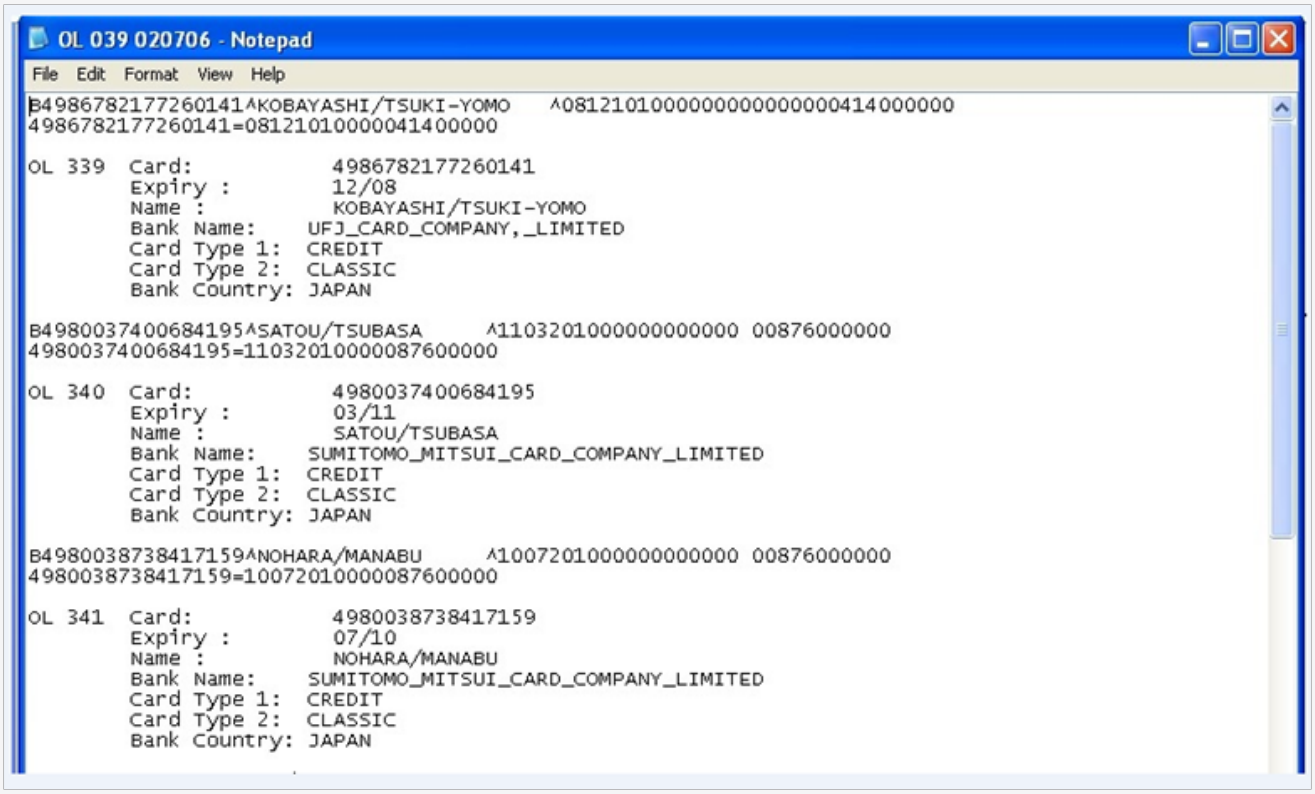


Figure 5: File showing credit card details of foreigners.

Conclusion and strategies for defeating identity thieves

This paper discusses in detail the finer points of the two-pronged strategy of prevention and cure. This article is focuses on the measures to be taken if a person's identity has already been compromised. While prevention is always better than cure, the key to surviving an identity theft is taking effective steps to minimize the damage by carrying out specific actions in a timely

How to cite this article: Mukesh S, Shailendra J. Digital Data Stealing from ATM using Data Skimmers: Challenge to the Forensic Examiner. J Forensic Sci & Criminal Inves. 2017; 1(4): 555567.

manner. The importance of keeping one's presence of mind and acting swiftly to effectively defeat one's identity thief is perhaps best demonstrated. The precautions that should be taken to prevent being a victim of identity theft can broadly be classified into two categories based on the type of transaction: offline transactions and online transactions. In Figure 6, illustrates the frequency and distribution of different personal information acquisition techniques in the United States, based on a survey conducted in 2006. Identity theft is often regarded as a high-tech crime [9-10]. One must monitor his/her credit reports thoroughly and regularly. We should cover the keypad while entering the PIN on an ATM. One must be aware that stand alone ATMs in convenience stores may be more susceptible to fraud than bank-based ATMs.

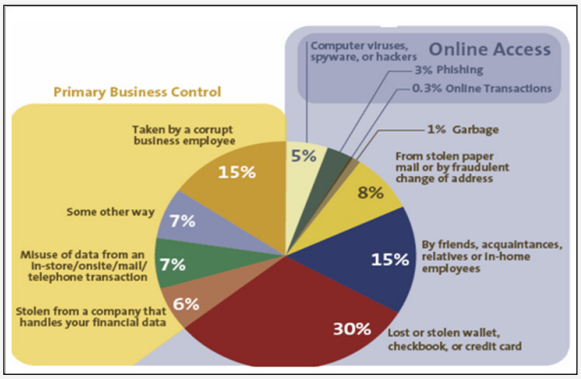


Figure 6: Victims who knew how their information was obtained.

According to The Federal Reserve, card fraud losses on any type of USA cards totaled $5.33 billion in 2012, up by 14.5% from 2011, with card fraud losses on debit cards at $1.57 billion in 2012. The USA card issuers lost $3.41 billion, equivalent to 6.7 basis points and 63% of the total card fraud in the USA while the card fraud losses of the merchants accounted for the other 36% [3]. So, we should aware from the close one also, during transactions. The scale and changing profile of card fraud underlines the urgency of implementing comprehensive security measures and of reinforcing those measures through use of the right fraud tools. So should developed intelligent fraud detection systems to determined and well-resourced criminals, those can manage to bypass new security techniques, so it is essential that even the strongest types of security are underpinned.

References

1. Consumer Sentinel Network Data Book (2008) Federal Trade Commission 2009, USA.
2. 10 Measures to Reduce Credit Card Fraud for Internet Merchants. Fraud Labs, Malaysia.
3. Payments Industry Intelligence (2017) Card Fraud Report - 2015.
4. John M Harrison (2003) The Growing Problem of Identity Theft and its Relationship to the Fair Credit Reporting Act. US Senate Banking Committee on Banking, Housing & Urban Affairs, USA.
5. US Attorney Office (2006) Western District of Michigan, Press Release, USA.
6. The Nilson Report (2017) California, USA.
7. Bob Mims (2006) Id Theft is the No. 1 Runaway U.S. Crime. The Salt Lake Tribune.
8. Dennis Romboy (2005) Meth Addicts Stealing Mail. Deseret News Utah.
9. (2004) Government Accounting Office, Social Security Numbers: Government could do more to Reduce Display in Public Records and on Identity Cards, USA.
10. Rennay Craats (2005) Identity Theft: the scary new crime that targets all of us. Altitude Publishing Canada Limited.