Skimming the Surface

How Skimmer Fraud Has Become a Global Epidemic

A research paper by Dr. Darren R. Hayes of Pace University sponsored by ACCA USA
February 14, 2014

Table of Contents

I. Acknowledgements

ACCA USA

This report would not have been possible without the Association of Chartered Certified Accountants USA. The ACCA is not only a world-renowned global body for professional accountants but is committed to raising public awareness about important issues relating to crime and providing solutions. Darren Hayes and Pace University would like to thank the generous support of this organization. In particular, we would like to acknowledge the following people at ACCA USA for their guidance and leadership on the project: Warner Johnston, Head of ACCA USA, Ruth Fasoldt, Business Development Officer and Sujata Adamson-Mohan, Engagement Manager. I would also like to acknowledge Faye Chua, Head of Future Research, ACCA Global.

European ATM Security Team (EAST)

EAST is an organization that has been a tremendous resource when conducting this research. The organization is committed to raising public awareness about skimmer fraud. EAST also facilitates knowledge-sharing amongst law enforcement agencies, private investigators, reporting agencies monitoring crime and implementing best practices, as well as other industry partners, who have made great strides to thwart criminal activity and reduce losses. I would like to especially acknowledge Lachlan Gunn, Coordinator, European ATM Security Team Ltd. (EAST Director) who provided introductions to key contributors across Europe and beyond. These contributors include (in no particular order of preference): Martine Hemmerijckx, Head of Service Disputes & Fraud, ATOS Worldline Belgium (EAST Director); Susanne Kreuzer, Security Management Payment Cards, EURO Kartensysteme GmbH (EAST Director); M. François Chane, Expert Sécurité, Risk Management & Audit, Groupement des Cartes Bancaires (EAST Member); Mark Sullivan, Director, Fraud Programs, Interac Association (East Member); Otto de Jong, Fraud & Security Consultant, ING DB (East Member); Úna Dillon, Head of Card Services & Communications, IPSO Ltd. (EAST Director); Erica McKinney, Member Services, IPSO Ltd. (EAST Member); Ari Partanen, Head of Service Production, Automatia Pankkiautomaatit Oy, Finland (EAST Director); Veronica Borgogna, Processi e Controlli, Coordinatore, Consorzio BANCOMAT (EAST Member); Claudia Talone, Processi e Controlli, Consorzio BANCOMAT; Giorgio Dorkin, Sviluppo e Standard, Coordinatore, Consorzio BANCOMAT; Leslie Stevens, Manager, Intelligence Unit, Canadian Bankers Association and Brian Underhill, Director, CELT Ltd. Last, and certainly not least, is Nick Webber, Director, CELT Ltd., has spent many hours educating me about how skimmer fraud schemes are perpetrated. I appreciate his dedication and patience.

Law Enforcement

My sincere thanks to those in law enforcement, who work tirelessly to bring skimmer fraud criminals to justice. They are a major deterrent to the perpetrators of skimmer fraud. The United States Secret Service is well known for their service in protecting the President of the United States, Vice-President and their families. However, they have been protecting the public from fraud since the nineteenth century. They are one of the world's foremost authorities on investigating skimmer fraud and, in fact, all types of financial fraud. Their investigative expertise is exemplary and their coordination with other agencies across the globe is commendable. I also wish to extend my gratitude to Bundeskriminalamt (BKA), Weisbaden, Germany, for their tremendous support.

Pace University

I appreciate the leadership provided Dr. Stephen J. Friedman, President of Pace University, who is an inspirational voice for justice in the community. I would like to extend my gratitude to Eric Morrissey, Director, Government & Community Relations, Pace University, who introduced me to ACCA USA and helped to make this report possible. Special thanks to Dr. Amar Gupta, Dean of the Seidenberg School of Computer Science and Information Systems at Pace University. My thanks to Dr. Catherine Dwyer, Chair of Information Technology, Pace University, who has continually supported my research endeavors. Roman Perez, Student, Pace University, has been both a marvelous researcher and a distinguished practitioner in security and computer forensics.

Other Notable Contributors

My sincere thanks to other invaluable contributors to this research, who include Dave O'Reilly, Chief Technologist, FTR Solutions, Ireland; Deborah Spidle, Director of EMV Solutions, Paragon Application Systems; Martina Costello, Information Security Manager, AIB Bank; Denis Heneghan, Head of Fraud Prevention, AIB Bank; and my good friend Bernadette Gleason, Second Vice President, High Technology Crime Investigation Association.

II. Purpose of the Research

Skimmer fraud is a worldwide epidemic but there have been no comprehensive worldwide studies completed on this important topic. A worldwide perspective is critical because many of the criminals who perpetrate this crime have accomplices across the world. It is also imperative to differentiate skimmer fraud from other forms of payment card fraud. Skimmer fraud involves the installation of an electronic device to "skim" data from the magnetic stripe on a payment card. The Target breach, for example, was as a result of hacking and these types of network breaches require a very different skillset and possess a dissimilar criminal profile.

Focus of the Research

Existing research in skimmer fraud is generally limited by industry. For example, there are groups that focus on producing information and statistics relating to ATM security and fraud. Additionally, there are other groups that focus on payment card fraud. We know of no institutions that produce comprehensive research on "skimmer fraud" as a concept that impacts the ATM industry, retailers, restaurants, energy, transportation and a variety of other industries. Therefore, this research is not industry-specific but is focused on a particular device (skimmer) within the realm of payment card fraud.

Importance of the Research

According to the 2013 Norton Report, the global cost of cybercrime rose to $113 billion (up from $110 billion), with an average cost per victim of $298 (up from $197 in 2012).[1] A significant portion of that cost involves payment card fraud. Estimates indicate that payment card fraud costs the United States $8.6 billion annually.[2] A Q3 2012 ACI Worldwide study of 5,223 consumers in 17 countries reported that a staggering 27% of payment card holders (debit, credit and prepaid)

[1] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013
[2] Aite Group report (2011)

experienced card fraud over the past 5 years.[3] It is therefore important to understand that a major contributor to this type of fraud – payment card skimmers.

Timeliness of the Research

The timeliness of this report cannot be underestimated as the credit card companies have instituted a liability shift to non-EMV compliant countries. The United States, as the largest ATM service provider in the world, will either suffer immense losses from skimmer fraud or comply with new directives provided by Discover, Visa, MasterCard and American Express.

Skimmer fraud is a huge problem in the United States and throughout the world. The Aite Group, Boston, Massachusetts, has reported that in 2010 the average loss from skimming crime was $30,000 and by 2011 that number rose to $50,000. The United States has been ranked number one in the world in terms of financial losses associated with skimmer fraud, in the first six months of 2011, followed by the Dominican Republic, Russia and Brazil, according to EAST's European Fraud Update[4].

Skimmer fraud shows no signs of subsiding but will continue to be a worldwide epidemic in the near term. A 2014 report about British tourists being targeted across Europe in a card cloning scam of up to £150 million illustrates how criminals continue to reap enormous profits from skimmer fraud.[5] In January 2014, thirteen men were indicted by the New York County District Attorney for using Bluetooth-enabled skimmers to steal more than $2 million from gasoline (petrol) stations in the United States. A recent Ipsos/Reuters poll reported that one in three Americans have noticed fraudulent charges appear on their credit or debit card statements and only 38% of Americans reported that their personal information had never been stolen.[6]

III. Executive Summary

Payment card fraud is a global crime costing financial institutions and retailers billions of dollars annually. A major component of payment card fraud is skimmer fraud. This scam involves the data from payment cards being captured with a "skimming device" and then the stolen card data is used to cash out those cards.

Role of the United States in Skimmer Fraud

The role of the United States is pivotal for criminal gangs because it has more ATMs than any other country and because it is not EMV-compliant (cards do not contain a global chip). Therefore, its non-EMV cards can be easily skimmed and then cloned. Cards that are cloned by criminals are also used in other non-EMV countries, like Ghana, Costa Rica, Mexico and Malta.

---

[3] "Global Consumers React to Rising Fraud: Beware Back of Wallet", Aite Group, October 2012.
[4] http://www.atmmarketplace.com/article/187133/EAST-publishes-third-European-fraud-update-for-2011?rc_id=30
[5] http://www.dailymail.co.uk/news/article-64501/British-tourists-hit-150m-credit-card-scam.html
[6] http://articles.chicagotribune.com/2014-01-27/news/sns-rt-us-datasecurity-poll-20140127_1_data-theft-payment-card-data-recent-data-breach

Law Enforcement Collaboration and Coordination

This research will show why collaboration between the United States, Europe and other countries is imperative when taking down these criminal gangs, which maintain a highly-organized global reach. In particular, the United States Secret Services works closely with law enforcement throughout Europe and these coordinated efforts are managed through Europol. Europol enables a swift response to skimmer fraud incidents. Law enforcement from the countries where these criminals reside have supported the coordination of criminal arrests; in some situations more than a hundred law enforcement agents have simultaneously coordinated arrests in a number of countries across Europe and even beyond.

Skimming Devices have Become More Advanced

Eastern European criminal gangs have, over the past few years, developed skimming devices that are much smaller but have greater memory. Additionally, these devices often incorporate advanced methods of encryption that can be problematic to decrypt. A number of sources in law enforcement believe that many of the advanced skills used in the development and deployment of skimmers were acquired at university level. Ubiquitous advances in technology mean that skimmers and their accessories have become much smaller. For example, smaller batteries, with more power, are now available to criminals. Sometimes a criminal may take a small battery from a remote-controlled toy helicopter to power a small skimmer. Years ago, a criminal would need to rely on shoulder surfing to acquire a customer PIN at an ATM or in some cases a larger handheld video camera. Today, a camera can be the size of a pen and be relatively inexpensive. These changes mean that skimmers today are faster to install, harder to detect and store more payment card information. Moreover, the use of Bluetooth means that the criminal can retrieve skimmed card data without physically removing the skimming device.

Skimmer Fraud Differs from Country to Country

Skimmer fraud in the United States is certainly different from countries in the European Union (EU) because of EMV. Interestingly, within EU countries there are notable differences. For example, in Ireland, there are only two manufacturers of ATMs and there are no non-bank ATMs. There have been very few incidents of petrol pump skimmer incidents or point-of-sale skimmers found. Increased vigilance by police, the use of anti-skimming devices and more attended petrol pumps have yielded tremendous success. The skimmer fraud landscape in Germany appears to be very similar. In contrast, in France, petrol pump skimmers appear to be a relatively new problem and this is probably due to the number of unattended petrol pumps.

ATM manufacturers are different from country to country, which impacts skimmer fraud. Interestingly, in Finland, ATMs have two card slots – one slot for cards with a global chip (EMV) and one for non-EMV payment cards.

There are ATMs in the United States with motorized card slots but very often the customer uses a dip reader. This makes a very big difference when it comes to the creation of skimming devices by criminals. In the United States, a criminal may physically hack off a dip reader and later use that dip reader to create a mold. The mold will in turn be used to make overlays to house skimmers. In the EU, where there are more motorized card slots, criminals can simply add a small skimmer at the front of the card slot.

The ownership and location of ATMs in the United States is very different from other countries. Out of the 425,000 ATMs in the United States, 222,500 ATMs are not deployed by financial institutions.[7] Furthermore, the vast majority of these ATMs are located off-premise (290,000 ATMs). Non-bank ATMs have thrived in the United States for many years, since ATM surcharges were recognized as a legitimate cost in 1996. Independent ATM deployers (IADs) do not exist in many other countries.

The use of handheld skimmers in the United States is a serious problem but in a number of European countries handheld skimmers are not an issue. One reason may be because at restaurants in the United States, the waiter or waitress takes your credit or debit card for a number of minutes and then returns later with a receipt. At restaurants in Europe, your payment card remains in your sight at all times; the waiter or waitress brings a terminal to your table, you enter your card into the machine and then enter your PIN. Your receipt is then handed to you. Therefore, it would be difficult for restaurant staff to skim your payment card. In 2011, the New York County District Attorney announced the indictment of restaurant staff from a number of New York City high-end restaurants who were using handheld skimmers.

Profiling the Skimmer Fraud Criminals

This research found that of the majority of criminals involved in skimmer fraud in the United States and Europe have come from Romania and Bulgaria. The problem is that unemployment is relatively high in these countries and therefore many unemployed electricians or electronic engineering graduates are recruited by gangs, who already have a portfolio of criminal activities that can include car theft, narcotics and burglary. The excellent education system in these countries means that many of these recruits make ideal skimmer fraud recruits. Not only have these criminals introduced advanced methods of encryption into the skimmers but they have found ways to circumvent sophisticated anti-skimming technologies.

Skimmer fraud is a fast way for criminals to earn cash but it is not just Eastern Europeans who have been involved in these activities. Many other ethnicities have perpetrated these crimes and the proceeds of skimmer fraud have been used for many different purposes, including funding terrorism.

Payment Card Fraud has Changed in EMV-Compliant Countries

When the United States adopts the use of chip and PIN payment cards (EMV) then skimmer fraud will dramatically decline but criminal activity will manifest itself in a different way. In many EMV-compliant countries, skimmer fraud has significantly declined but physical attacks have increased. A physical attack could be a gas attack, a bomb or a truck used to physically rip out the ATM. Other schemes like card trapping, cash trapping, transaction reversal fraud and currency fishing are also on the increase in a number of countries in the European Union and we should anticipate similar challenges in the United States with the introduction of EMV. It is important to understand that new physical attacks can cost an organization a lot more in damages than in the initial loss of cash. For example, a card trapping device may yield €100 to the criminal but the damaged ATM may cost €2,000 to repair.

[7] http://natmc.org/documents/2012/10/about-the-atm-industry.pdf

Geo-blocking Makes a Difference

Some countries have dramatically reduced payment card fraud by imposing restrictions on where geographically a card can be used. Obviously, this type of move can be initially very unpopular with bank customers but these programs have deterred criminals, as noted in the successful implementation of regional blocking in The Netherlands and in Belgium. Some banks in Germany have instituted regional blocking and losses from skimmer fraud have been further reduced by limiting the amount that a customer may withdraw at a foreign ATM. Regional blocking could be introduced by banks in the United States to limit fraud; only one third of United States citizens possess a passport.[8]

Windows XP is the New Challenge

18% of ATMs in the United States are a decade or older, which poses a notable obstacle to switching over to EMV-compliant ATMs. Many ATMs today run on Windows XP and support for this operating system ends on April 8, 2014. This means that there will be no more security updates to patch potential vulnerabilities. Therefore ATMs in the United States face a new threat in addition to skimmer fraud.

Future of ATM Transactions

Given the size and scope of skimmer fraud, there are numerous debates about the future of ATM transactions. Some have debated the use of new technologies, like smartphones and Near Field Communication (NFC) or the use of biometric authentication. Some countries use biometric authentication at ATMs but the overarching issue is that you cannot replace a biometric if it is stolen. There is no consensus on future technologies to prevent ATM skimmer fraud except for the introduction of EMV payment cards.

Preventing Skimmer Fraud

Interestingly, skimmer fraud can often be easily detected. There are cards that bank employees can use to see if a POS terminal has been tampered with or to detect if a skimmer has been installed onto an ATM card slot. The general public can be an extension of law enforcement. Consumers need to be made aware of how to recognize skimming scams and be provided with instructions about how they can alert ATM owners.

IV. Research Methodology

This research was conducted over a 15 month period. To provide a more comprehensive review of skimmer fraud worldwide, Darren Hayes travelled extensively across the United States and Europe and interviewed staff from crime labs of financial institutions, local and federal law enforcement, skimmer device examiners, representatives from the payment card industry, fraud research firms and financial regulators. Hayes attended also attended conferences, related to financial fraud, in the United States and Europe.

In the United States, skimmer fraud statistics were largely unavailable because there is no central repository or agency responsible for collecting this data. Some countries have reliable, detailed

[8] http://www.forbes.com/sites/andrewbender/2012/01/30/record-number-of-americans-now-hold-passports/

statistics but other countries do not have a central reporting system. Where available, statistics are provided on a country-by-country basis. Skimmer fraud statistics for emerging economies, including Brazil and China, are necessary to provide a more comprehensive worldwide perspective but unfortunately those statistics were unavailable.

V. Skimmer Fraud Technologies

A skimmer is an electronic device, which is used to read and store electronic data. There are many different types of skimmers including radio frequency identification (RFID) skimmers that are often used to fraudulently read data from RFID tags embedded in US driver licenses and US passports. However, this research focuses specifically on the use of skimming devices that read and record data from consumer payment cards (ATM, credit, debit, prepaid and electronic gift cards). The types of skimmers used with payment cards, discussed in this research, include the following:

A. Overlay devices (Automated Teller Machine, Gas Station Pump and Ticket Vending Machine Skimmers)
B. Parasite devices (Point-Of-Sale Terminal Skimmers)
C. Handheld Skimmers (Restaurant/Retailer Skimmers)

VI. The Automated Teller Machine (ATM)

History of the ATM

There is some confusion and controversy surrounding who the actual inventor of the ATM was. In 1962, Luther George Simjian developed the precursor to the modern day ATM. Introduced in New York, this device was an automated cash deposit machine but the technology was later abandoned due to limited demand.

In May 1966, James Goodfellow patented the Personal Identification Number (PIN) in Great Britain. There are many who credit John Shepherd-Baron with the development of the first ATM. In 1967, the De La Rue Automatic Cash System was rolled out in in a Barclay's Bank branch in North London, U.K.[9] This ATM enabled the withdrawal of cash with the input of a radioactive Carbon-14 paper by the customer. Shortly after, the Bankomat was unveiled in Sweden and this automated cash dispensing unit enabled customers to withdraw cash with a plastic card that contained an encoded serial number.

In July 1967, the Chubb MD_2 was introduced in Great Britain and this automated cash dispenser used a plastic perforated card and used a PIN for authentication. In 1969, the Total Teller System was unveiled in the United States and required the user to have a magnetic card – similar to what is used today. Introduced in 1984, the NCR 5070 was developed in Scotland and was the first fully functional ATM – meaning that it facilitated transfers, printed statements, deposits and withdrawals. In 1994, the Triton 9500 entered the market as the first low-end, non-bank ATM. In

[9] http://www.atminventor.com/

2010, the first biometric ATM was installed in Poland.[10] The first Bitcoin ATM was unveiled at a coffee shop in Vancouver in 2013.[11] This ATM converts Bitcoin to Canadian dollars and vice versa.

There are 2.2 million ATMs installed worldwide and a new ATM is installed every 5 minutes, according to Retail Banking Research.[12] They also estimate that there will be more than 3 million by 2016.[13] North America is the largest ATM market in the world. The United States has the largest number of ATMs – approximately 425,000[14]. In the United States there are approximately 14 billion cash transactions conducted annually.[15]

There are numerous ATM manufacturers, which include the following:

- NCR
- Triton
- Wincor Nixdorf
- Diebold
- KORO-16
- Fujitsu
- SIGMA
- KEBA AG

The brand of ATM will differ from country to country. For example, Diebold is virtually non-existent in Ireland and the U.K, whereas they are a major manufacturer in the United States. Also, ATMs in much of Europe will have a motorized card slot and not a slot for dipping and quickly removing the customer card; in other words, the ATM holds the card during the transaction. This means that card trapping is possible with these types of ATMs while this is not the case with a slot used for dipping and quickly removing the card. Furthermore, non-bank ATMs do not exist in all countries; in the United States, for example, non-bank ATMs are widespread and appear in delicatessens, casinos, airports and other non-bank locations. Interestingly, there are more independent ATM deployers (IADs) in the United States (222,500 ATMs) than ATMs deployed by financial institutions (202,500 ATMs).[16] 290,000 ATMs are off-premise versus 135,000 ATMs that are on-premise. Therefore, it is important to remember that the ATM landscape varies greatly from country to country, which in turn impacts how skimming crimes are perpetrated.

ATM Skimmers

One of the most common types of skimmer is the ATM skimmer, which is used to record the data contained on the magnetic stripe on the back of a consumer's ATM card. A skimmer may be placed on a stand-alone ATM, such as the ATMs seen at convenience stores, or at banking locations. At a bank ATM, card data is recorded in one of two possible locations: (1) doorway to the bank ATM

[10] Cash Box: The Invention and Globalization of the ATM, ATMmarketplace.com
[11] http://www.cbc.ca/news/technology/world-s-first-bitcoin-atm-opens-in-vancouver-1.2286877
[12] http://www.rbrlondon.com/
[13] "Global ATM Market and Forecasts to 2016." Retail Banking Research. September 2011.
[14] http://natmc.org/documents/2012/10/about-the-atm-industry.pdf
[15] http://www.diebold.com/atmsecurity/files/DBD_ATMFraud_WP.pdf
[16] http://natmc.org/documents/2012/10/about-the-atm-industry.pdf

where the user is required to use their card to gain entry or (2) an overlay device installed on the actual ATM. **Figure 1** shows an actual skimmer recovered from an ATM.

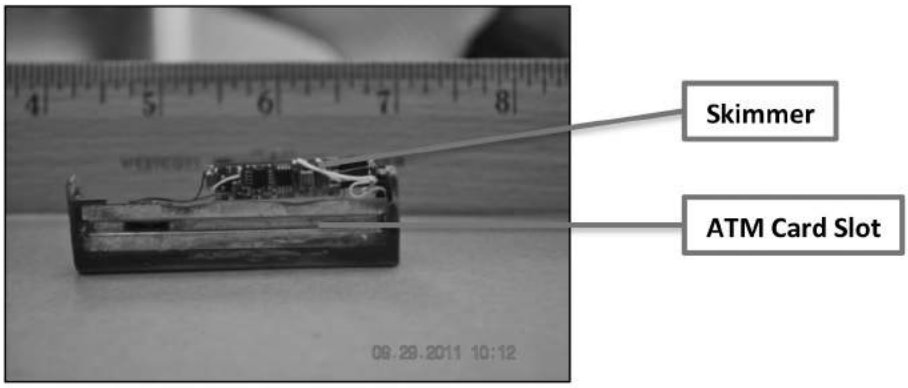

Figure 1. ATM Card Slot Skimmer

Figure 2 shows a motorized card reader from an ATM with a skimmer placed below the card reader. As you can see from the image, once the skimmer is placed onto the card slot it is difficult to spot.

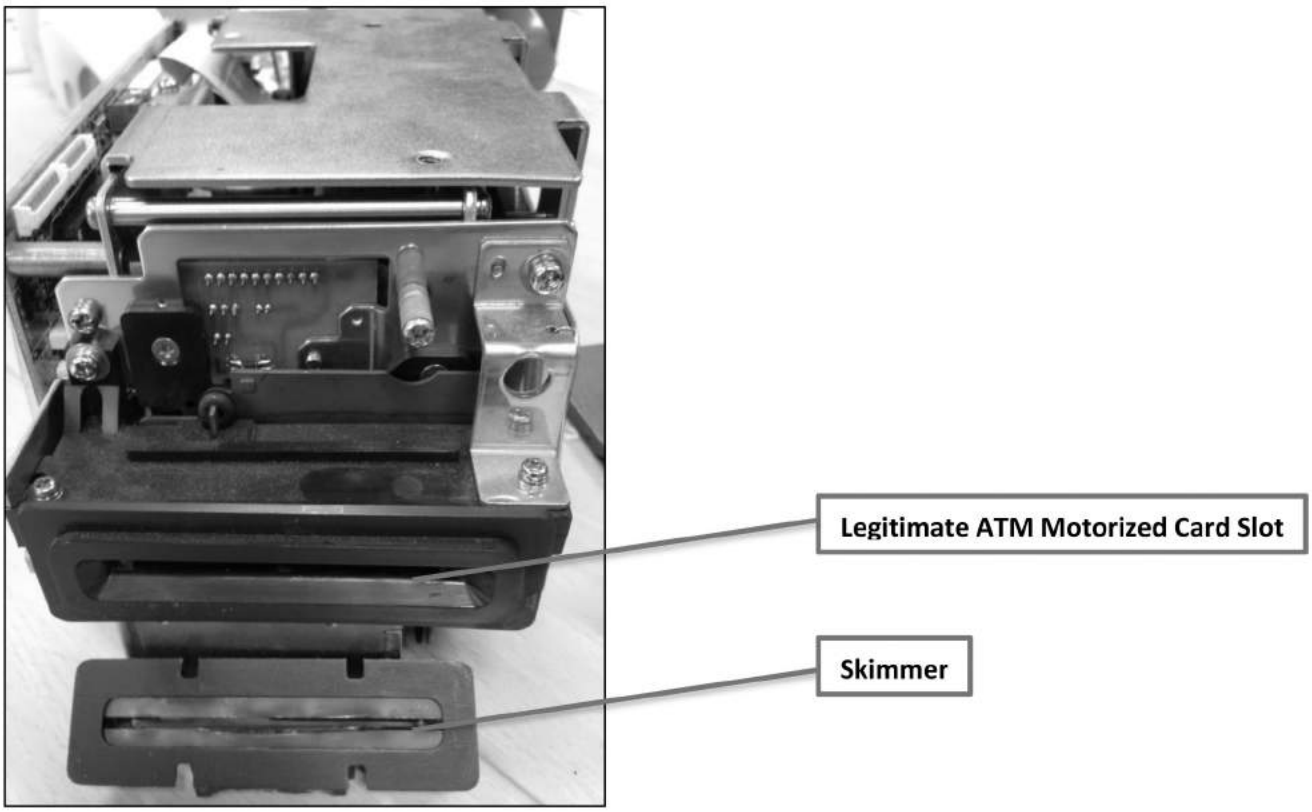

Figure 2 Motorized Card Reader from ATM with Skimmer Placed Below

In some cases, an entire false fascia will be added to the ATM as shown in **Figures 3** and **4**. These overlays were recovered by police in Europe.

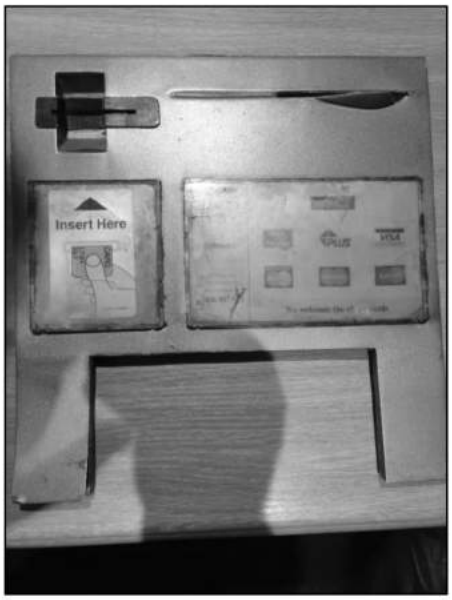

Figure 3 False ATM Overlay

Figure 4 ATM False Overlay

Figure 5 below shows the components associated with a skimmer installed by a criminal. Pictured on the underside of the overlay is a circuit board from a commercial magnetic stripe reader, which is taped to the back of the ATM overlay. This is connected to a Bluetooth transmitter circuit board, which is also taped to the ATM overlay. The antenna for the Bluetooth transmitted is also taped to the overlay and pictured above the printed circuit board (PCB). Both are powered by Nokia cellphone batteries. The unit on the right is a Bluetooth receiver circuit board with an antenna at

the top connected to a portable serial data recorder. The ATM panel transmits magnetic stripe data direct to the portable serial data recorder (pictured on the right side of the picture) as payment cards pass through the false ATM panel. Customer PINs are captured using a wireless camera connected to a wireless video receiver – both of which are battery-powered.

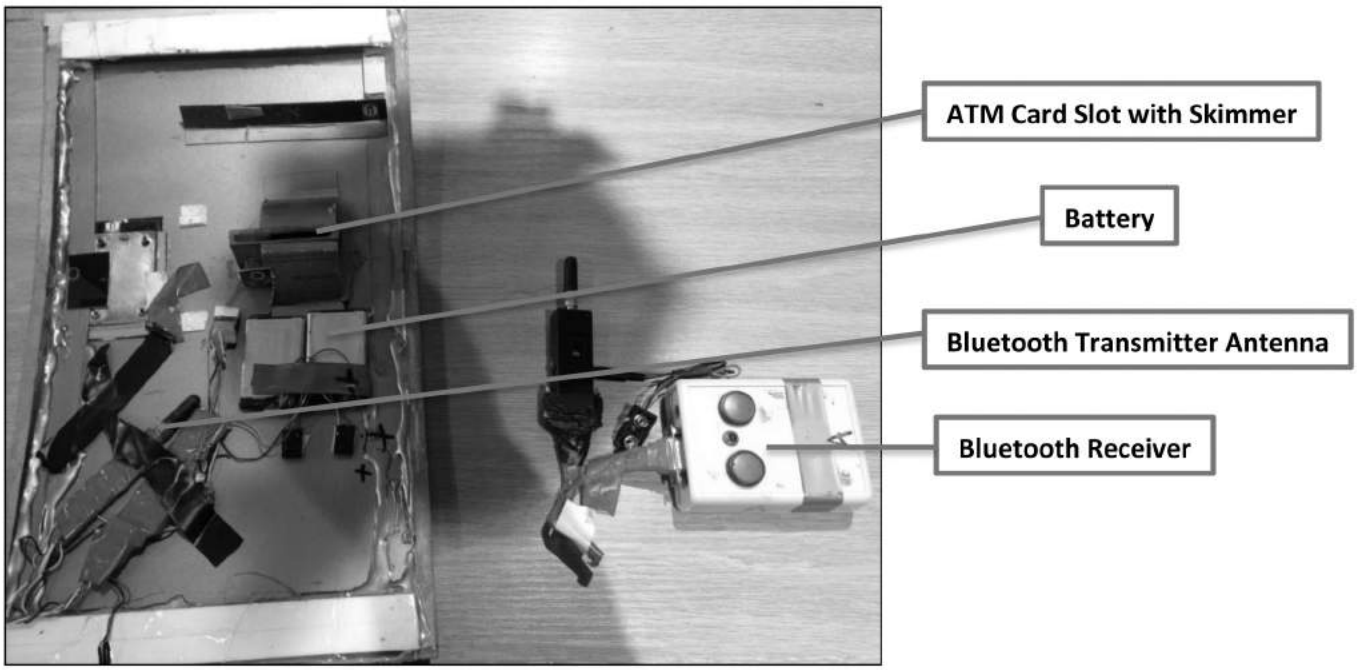

Figure 5 Underside of ATM Overlay

SMAG DC Skimmer

Around 1999, the SMAG DC skimmer appeared in the United States. This skimming device cost around $500 and could store data from 80 payment cards.

ATM skimmers can be purchased from numerous different sources online. They typically store data from more than 200 cards. There are many Websites that facilitate the sale of skimmers and, as you can see from **Figure 6**, ebay.com is one such site.

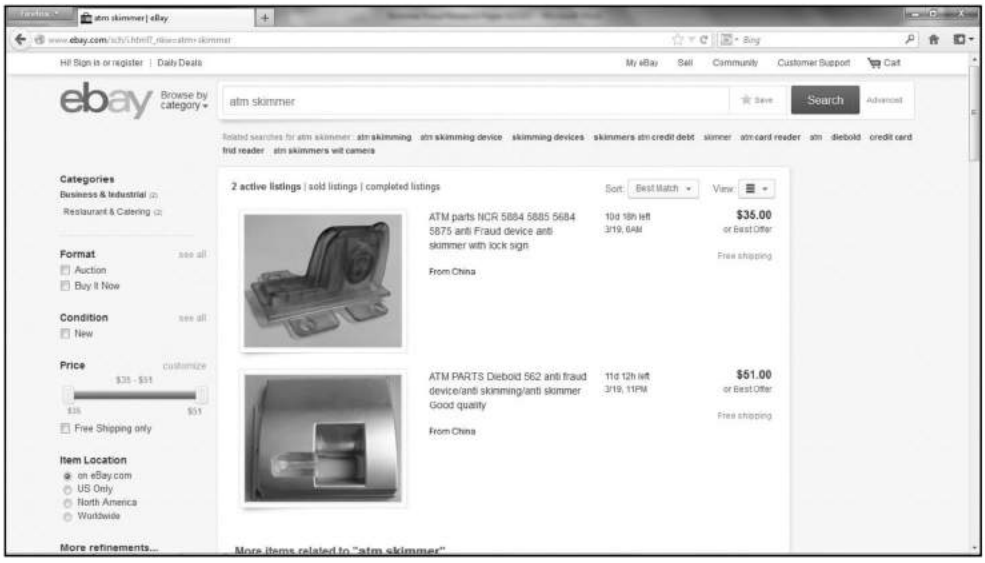

Figure 6 ATM Skimmer Parts for Sale on ebay

The most well-known, or some would say the most "notorious", Website for purchasing skimmers is CardReaderFactory (www.cardreaderfactory.com). The Website does not call these devices "skimmers" but instead refers to the devices that they sell as "magnetic stripe readers". **Figure 7** shows some of the devices that the Website sells.

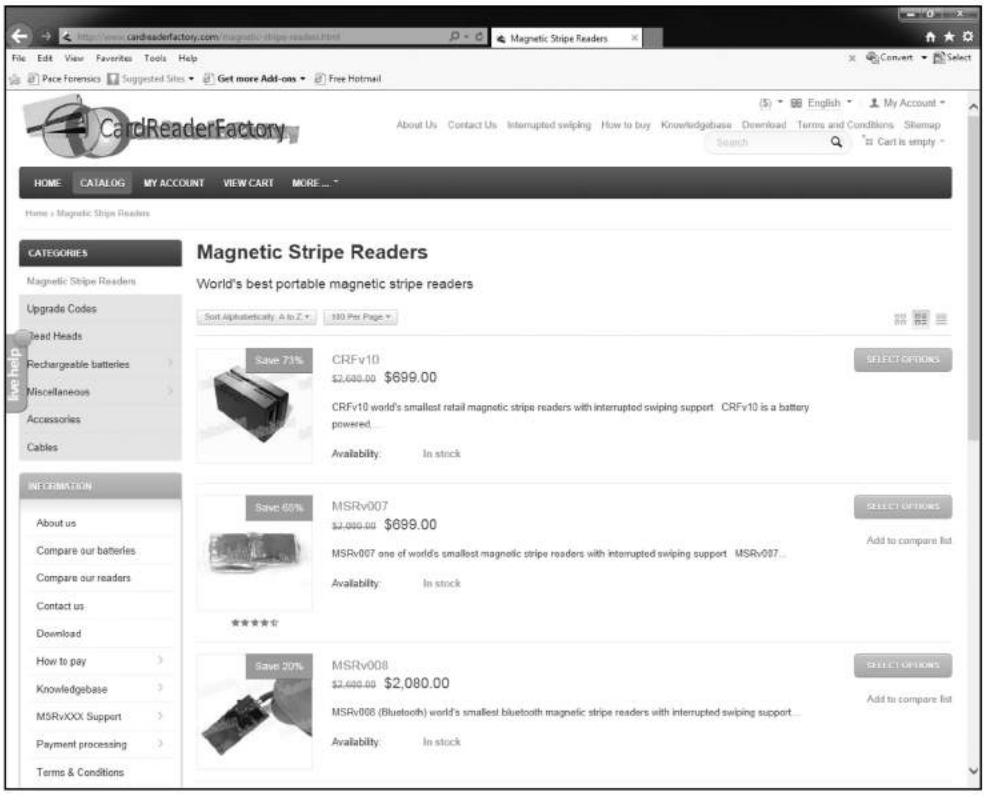

Figure 7 CardReaderFactory "Magnetic Stripe Readers" For Sale

Card Trapping

The European ATM Security Team (EAST)[17] has noted another ATM scam, which is referred to as "card trapping". This type of fraud is not as common though. A device is installed to trap a user's ATM card, which can only be retrieved by the perpetrator, along with a compromised user PIN. iPods with a camera feature have sometimes been used to capture the PIN due to battery efficiency and storage capacity. The difficulties associated with cloning EMV cards has made card trapping a better prospect for thieves. EAST reported a 216% increase in card trapping in the first six months of 2012.[18]

Card trapping, cash trapping, currency fishing and transaction reversal fraud are not skimming scams but are important to mention. The introduction of cards with an EMV chip has resulted in a dramatic decline in skimmer fraud but has recently prompted changes in ATM fraud.

Lebanese Loop

One of the earliest card trapping scams was the Lebanese Loop. The name is derived from the ethnicity of the criminals that used these initially. With the Lebanese Loop, the criminal inserts a transparent plastic sleeve. When an unsuspecting customer inserts his card into the motorized slot and enters the PIN, the ATM cannot read the magnetic stripe on the card and an error message displays. When the customer then tries to retrieve the card he cannot because the sleeve is designed to trap the card and is not returned to the user. The customer does not suspect that anything has gone awry and simply walks away. The criminal then returns and retrieves the sleeve with the card and then uses that stolen card to fraudulently withdraw the customer's funds.

There are other card trapping scams that have been used in the past, including the Builders Loop, Romanian Loop, the Algerian V, Floss Loop and Wire Loop.

Cash Trapping

Also referred to as currency trapping, this ATM strategy is similar to card trapping but, instead of trapping a card, a false dispenser front is installed to trap cash. With 99% of ATMs in Europe being EMV-compliant, this type of crime has increased dramatically while skimming has actually been declining. In the first six months of 2011 there were 6,756 reported cases with losses totaling €495,782 compared to 150 reported cases during the first half of 2010. What is important to note is that even though the transaction loss may only be €200 per incident with this type of fraud the cost to fix the damaged ATM may be €2,000.

Currency Fishing

This fraud involves a criminal installing hooks, wires or probes, which are hidden from the customer, and prevents cash from being dispensed or deposits being made. The perpetrator will then return to the ATM and use a fishing device to retrieve the cash and deposit envelopes.

Transaction Reversal Fraud (TRF)

This crime involves tricking an ATM into assuming that an error has occurred in a cash transaction, thereby resulting in an account not being debited. One method of TRF occurs when a device is

[17] www.european-atm-security.eu
[18] "European ATM Crime", EAST, 2012.

placed on the clips in an ATM, which separates currency bills being dispensed. When the transaction is not completed, the ATM believes that the cash has not been dispensed to the customer. In yet another scam, all of the notes are dispensed and the criminal carefully removes only some of the bills. After the process times out, the ATM retracts the remaining bills but is unable to count the bills and assumes that all of the bills have been returned to the ATM.

Approximately 65% of ATM crime involves card and cash trapping, and transaction reversal fraud with skimming only accounting for 35% of ATM crime, according to EAST.[19] According to EAST, there has been a significant increase in TRF, with the number of incidents, in the first half of 2012, reportedly 2,479 representing losses of approximately €1 million, compared to 41 cases representing €36,700 during the same period of 2011.[20]

ATM Skimmer Fraud Statistics (North America)

ATM Skimmer Fraud in United States

A recessionary economy appears to be a stumbling block for upgrading to new ATMs with integrated security improvements; a Q2 2011 Impact Report, by Aite Group, indicates that 18% of US banks still maintain ATMs that are a decade or older.[21] The survey of executives did, however, show that bank executives are more concerned about the threat of skimmers than ever before.

There is good news in this report however - banks are taking steps to mitigate the risk of skimmer fraud; surveyed executives estimated that by 2012, 45% of their institution's ATMs would have an anti-skimming solution, which is up from 40% in 2011 and 31% in 2010. What is of real concern is the fact that on April 8, 2014, Microsoft will end its support of Windows XP. This means that there will be no more security updates released for this operating system. The problem is that there are thousands of ATMs that run Windows XP, thereby rendering them vulnerable to attack. The ATM Industry Association has already issued a warning to its members about their concerns.[22]

According to the Verizon Data Breach Investigations Report 2012[23], ATM and gasoline station skimmers were responsible for a significant increase in physical breaches, representing 29% of these breaches. According to the Verizon Data Breach Investigations Report 2013[24], skimmers are responsible for almost all physical data breaches today.

ATM Skimmer Fraud in Canada

Canada has a population of about 35 million. Founded in 1994, Interac is a Canadian-based organization that facilitates electronic financial transactions through their national payment network. The organization was founded by CIBC, Royal Bank of Canada, Scotiabank, TD Bank and

---

[19] http://www.finextra.com/news/announcement.aspx?pressreleaseid=46645
[20] "European ATM Crime", EAST, 2012.
[21] "U.S. Bank ATMs: Self-Service Trends in a Challenging Economy", Aite Group, August 2011.
[22] http://www.atmmarketplace.com/article/226829/ATMIA-publishes-Windows-XP-risk-analysis?utm_source=NetWorld%20Alliance&utm_medium=email&utm_campaign=EMNAAMC01292014
[23] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-press_en_xg.pdf?__ct_return=1
[24] http://www.verizonenterprise.com/DBIR/2013/

Desjardins.[25] They manage 60,000 ATMs and 766,000 POS terminals throughout Canada.[26] Interac Association announced that all Interac acceptance devices must be EMV-compliant by December 31, 2015.[27] As of October 31, 2012, there are 73.9 million Visa and MasterCard payment cards in circulation in Canada.[28] In 2012, credit card fraud in Canada was $CAD 439.36 million, compared to $CAD 436.59 million in 2011.[29] However, Interac debit card fraud dropped 45%, from $CAD 70 million in 2011 to $CAD 38.5 million.[30] The notable decline in fraud is as a result of enhanced fraud detection analytics, increased law enforcement support and the introduction of EMV.

In 2009, debit card fraud in Canada was estimated to be $142 million, which subsequently declined to $119 million in 2010 and then fell to $70 million by 2011.[31] Visa and MasterCard implemented a domestic liability shift in the first half of 2011, which accounts for the dramatic decline in payment card fraud.

ATM Skimmer Fraud Statistics (Europe)

Skimmer fraud in Europe is different from the United States because of a number of factors. One factor is that ATMs in Europe are for the most part EMV-compliant. Another reason for differences in ATM fraud is that ATMs are often different in the United States. For example, there is a large number of non-bank ATMs in the United States, which are not found in every country. Moreover, Certain ATMs have certain vulnerabilities and the type of ATMs from country to country will vary greatly. According to a report by the European Central Bank (ECB) in July 2013, ATM fraud accounted for 20% of all payment card fraud (€232 million).[32] The report also states that 95% of counterfeit card fraud, related to ATM fraud, occurs outside of Europe.

ATM Skimmer Fraud in Ireland

Ireland has a population of approximately 4.58 million. According to the Irish Payment Services Organization (IPSO), in 2011 there were 194 skimming incidents, of which 142 were successful. During 2011, anti-skimming devices were installed on the majority of ATMs. Coupled with an anti-skimming initiative was more vigilance by banks and ATM maintenance workers. Additionally, there were some notable ATM fraud-related arrests by the Gardaí (Irish police). The outcome was that in 2012 there were only 13 ATM skimming incidents and 12 of those were successful. In 2013, there have been some successful ATM skimmer incidents where an anti-skimming device became inoperable or was incorrectly installed. An ATM skimmer that was found in Ireland in 2013 is arguably the first stereo skimmer in the world.[33] This find may indicate a new technical advancement for thieves. Most ATMs in Ireland are manufactured by NCR but there are also some Siemens Nixdorf machines. Diebold is virtually non-existent in Ireland and the U.K. All card readers

---

[25] http://www.canadabanks.net/default.aspx?article=Interac
[26] http://www.interac.ca/en/interac-about/about-us
[27] https://www.globalpaymentsinc.com/Canada/customerSupport/industryInit/chip_shift.html
[28] http://www.cba.ca/contents/files/statistics/stat_cc_db038_en.pdf
[29] http://www.cba.ca/contents/files/statistics/stat_creditcardfraud_en.pdf
[30] http://www.cba.ca/contents/files/statistics/stat_creditcardfraud_en.pdf
[31] www.atmmarketplace.com
[32] https://www.europol.europa.eu/content/international-network-latvian-payment-card-fraudsters-dismantled
[33] https://tmdsecurity.com/UserFiles/File/TMD%20RBR%20Bulletin052013.PDF

in Ireland are motorized as opposed to the United States where newer ATMs generally have dip readers.

ATM skimmers do account for the majority of skimmers but there are cases of skimmers being used at petrol stations. In 2012, according to IPSO, there were 15 skimmers found at fuel pumps. It appears that these skimmers are less prevalent in Ireland and the U.K. than in Europe because there are far fewer unattended petrol stations in Ireland and the U.K. than in Continental Europe.

Handheld skimmers are rare and point-of-sale terminal skimmers have not been seen for a few years now because of chip and PIN (EMV).

ATM Skimmer Fraud in France

According to Banque de France, law enforcement recorded a significant decline in credit card fraud in 2012.[34] In 2012, there were 122 people arrested, compared with 234 people in 2011 and 235 in 2010. This decline has been interpreted as the result of more severe sentences for those convicted of payment card fraud. Another reason for the decline is that credit cards issued in France require that the user have a PIN associated with that card; typically only debit and ATM payment cards require a PIN. Nevertheless, skimmer fraud recorded a notable increase in 2012; there were 1,100 skimming attacks, compared with 634 in 2011, 527 in 2010, 526 in 2009, 427 in 2008, 411 in 2007, 526 in 2006 and 200 in 2005.

The Banque de France report also shows that point-of-sale skimming incidents were 26 in 2012, compared to 32 incidents in 2010. In 2012 there were 28 incidents of petrol station skimmers, compared to no incidents in 2011. Some analysts have indicated that there are more unattended petrol pumps in France, which may account for more instances of petrol pump skimmers.

ATM Skimmer Fraud in Italy

ATM manufacturers vary from country to country but in Italy the following companies produce Bancomats (ATMs):

- NCR
- Wincor
- Diebold
- SIGMA

In terms of POS, Ingenico, Verifone and Pax manufacture these devices. Gas pump card readers are manufactured by Gilbarco, Globalcom and Tokheim in Italy.

Consorzio BANCOMAT is the agency in Italy responsible for determining which organizations have the authority to operate in the payment services industry. They establish operational rules for ATM acquirers, including technical and security protocols. They also monitor payment card fraud in Italy; fraud data is collected via the organization's Website. Financial institutions register with Consorzio BANCOMAT and then notify them about incidents of fraud. When an acquirer notifies Consorzio BANCOMAT about an incident they can also enter a list of cards that were used on a

[34] http://www.banque-france.fr/observatoire/telechar/2013/Rapport-annuel-2012.pdf

compromised terminal. The system will identify and inform the issuer about the potential risk and the issuer in turn can monitor and, if necessary, block transactions associated with the flagged card. There are no non-bank ATMs in Italy, which is different from the United States.

According to Consorzio BANCOMAT, there are 33 million EMV-compliant payment cards in Italy and 1 million non-EMV compliant cards. Currently, BANCOMAT cards do not support contactless technology. The Italian Postal Police and the Carabinieri Police are primarily responsible for investigating skimmer fraud. Like other European Union countries, Italian banks and police work with Europol on investigations involving organized criminals operating in multiple nations.

ATM fraud in Italy is primarily instigated through skimming, card trapping and cash trapping. Skimming can occur at the doorway to the ATM but in most cases in Italy a skimmer will be placed on the actual ATM. A pinhole camera is usually added to the metal plate above the keypad to record the user's PIN. Cash trapping, using hooks, has occurred at a number of ATMs and there are only a few incidents of card trapping. Interestingly, cash trapping only occurs on a couple of different models of ATM. According to Consorzio BANCOMAT, in 2012, 75.45% of ATM fraud was cash trapping, while skimming only accounted for 21.28% of incidents. However, incidents of skimming fraud, during the first 10 months of 2013, accounted for 40% of ATM fraud and cash trapping declined to 59%.

It appears that cash trapping is on the decline, particularly during the second half of 2013, because of conscientious efforts to eradicate this type of fraud. Interestingly, there are notable differences in the types of ATMs that are attacked with one particular ATM brand being attacked the most (72.25%).

The largest number of skimming incidents occurred in the North of Italy (62.97%) and cash trapping in Northern Italy accounted for 66.3% of incidents. This might not be all that surprising given the greater diffusion in this area of electronic payment instruments and methods of cashless payment. Nevertheless, a higher percentage of ATM fraud does occur in Northern Italy.

In 2012, there were almost 11,000 cards produced, which were probably counterfeit, related to skimmer fraud in Italy. In the first 10 months of 2013, there were 14,000 cards utilized on ATMs with skimmers, which is a notable increase year-over-year.

Card trapping incidents are negligible for both 2012 and 2013. Card trapping makes use of motorized card slots at ATMs, which are prevalent in Italy and in other European countries.

Cash trapping is often a preferred method to access cash quickly given EMV-compliance. Many of the suspects arrested are from either Romania or Bulgaria. The data from cards skimmed in Italy are being duplicated and then cashed out in non-EMV compliant nations like the United States, countries in South America, Morocco and Malta.

ATM Skimmer Fraud in Germany

In Germany, there are very few non-bank ATMs. The following companies produce ATMs for use in Germany:

- Wincor Nixdorf
- NCR
- Diebold
- KEBA AG

ATMs in Germany have motorized card slots instead of dip readers. Problems associated with skimmers have prompted a number of banks to deactivate card-activated door openers. In Germany, the vast majority of ATMs are located in the lobbies of banks and not facing the street, which is different from other countries, where street-facing ATMs are also frequently found.

EURO Kartensysteme GmbH has a number of functions, which includes recording and reporting on skimmer fraud statistics for the banking industry. An interbank network exists in Germany, which is known as girocard. A German girocard is typically either a co-branded Visa card or Maestro/Cirrus (MasterCard). Germany has a population of about 80 million but 97 million girocards have been issued in the country – all of which are all EMV-compliant. There are 57,600 ATMs in Germany, which are all EMV-compliant. Additionally, there are 680,000 point-of-sale terminals, of which 95% are EMV-compliant.

Skimmer fraud has historically been relatively low in Germany. In 2004, there were 2,900 cases of skimmer fraud and this fraud reached its high-point in 2010 with 35,000 incidents. One could speculate that there was a dramatic increase during that year in anticipation of EMV being introduced to Germany in 2011. During 2011, there was a dramatic decline in skimmer fraud incidents, which totaled 21,000 for the year. The introduction of EMV has certainly brought a decline in skimmer fraud because the number of incidents in 2013 declined to 17,000. Not only have the number of occurrences fallen dramatically but the associated dollar losses have also dropped; in 2010, losses were €55 million compared to €12.5 million for 2013.

There may of course be other factors contributing to the relatively low rates of skimmer fraud. For example, one of Germany's major banks uses geo-blocking to prevent withdrawals from ATMs in other countries. If a customer wishes to travel abroad then he needs to apply to the issuing bank and obtain an additional payment card to be used abroad. Additionally, other banks have restrictions on the amount of a withdrawal at a foreign ATM – particularly for withdrawals in non-EMV-compliant countries, like the United States.

As mentioned, ATMs in Germany are generally located in lobby areas. The number of door opener skimmers found has diminished significantly, from 36 in 2010 to 8 in 2013. This decline is due to the fact that many banks have now disabled the card entry slots at ATM lobbies.

So what happens with cards that are skimmed in Germany? Like many other skimmed cards in Europe, the criminals are cashing out these cards in non-EMV compliant countries and the United States is number one, with 18% of cards being cashed out. Criminals are also taking those skimmed payment card numbers and traveling to Brazil (11%), Indonesia (11%), India (10%) and Thailand (9%) to cash out. These criminals have also been found in places like Costa Rica, Mexico and Ghana cashing out cards. The good news is that the average loss per payment card has declined from €1,623 in 2009 to €711 in 2013.

Compromised point-of-sale (POS) terminals are somewhat of an issue and these incidents have been on the rise in Germany. In 2010 there was 1 skimming incident but that number rose to 84 (24 of which resulted in losses) in 2013. In 2012, 50 terminals were compromised with losses in excess of €10 million. Losses from compromised POS terminals in 2013 dropped to €2.2 million.

There are very few instances of skimmers at petrol stations in Germany and this may be because there are very few unattended petrol (gasoline) pumps in the country; there were 2 occurrences of petrol station skimmers in 2013. Since 2011, losses from this type of skimmer fraud have only totaled €2.6 million.

There have only been one or two instances of ticket machine skimmers in Germany. The number of handheld skimmers found over the years is negligible. Since 2011, ticket machine losses from skimmers have only amounted to €327,000.

There are no biometric ATMs in Germany. Additionally, there are no smartphone applications that have been developed for cash withdrawals.

The following terminals are manufactured for use by German retailers:

- Ingenico
- Hypercom
- VeriFone

There are very few contactless cards in Germany but they are slowly growing in popularity. The Ingenico iPP350 is the first payment terminal approved in Germany for use with *girogo* – a contactless payment system. MasterCard's *PayPass* and Visa's *payWave* contactless payment protocols can also be found in Germany. Customers can use their contactless cards for smaller dollar transactions where the consumer does not need to enter a PIN or sign.

ATM Skimmer Fraud in Finland

Finland has a population of about 5.4 million. 99% of payment cards in the country are EMV-compliant. Automatia Pankkiautomaatit Oy is a bank-owned ATM company and all banks in Finland are customers of Automatia. The company operates bank ATMs and their networks in Finland. Kontanten AB is a Swedish company that operates ATMs independently of banks and other financial institutions, i.e. they provide non-bank ATMs in Finland. The company operates 1,000 ATMs in Sweden, Finland and Norway.

Skimmer fraud is not a major issue in Finland; in 2013 two skimmers were found installed on Automatia ATMs and three were found on Kontanten's ATMs and only two of these skimmers were successful (Kontanten ATM). Kontanten uses Wincor for its ATMs. There are only two brands of ATM in Finland, which are NCR and Wincor.

Of particular note is that Automatia's ATMs have a dual card reader – one for cards with an embedded EMV chip and another reader for chipless cards. These ATMs use a dip reader for EMV cards, which means that card trapping is not an issue in Finland. **Figure 8** shows an NCR Automatia in Finland, which was developed specially for the company.

Figure 8 Automatia ATM in Finland with 2 Card Slots

Older ATMs have a motorized card slot for non-EMV cards but the newer NCR (Automatia) ATMs use a dip reader for non-EMV cards. Regional blocking is used by some banks in Finland. There are no biometric ATMs in Finland.

In terms of POS skimmer incidents and petrol pump skimmers, there are a few instances of this fraud each year but the number of incidents is negligible. There were no handheld skimmer fraud incidents in 2013.

ATM Skimmer Fraud in Belgium

Belgium has a population of about 11 million. Belgium is different from other countries because banks made a decision not to invest in anti-skimming solutions. This is because anti-skimming devices have an average lifecycle of 1-2 years before these devices are circumvented by criminals. Instead, Belgian banks decided to institute regional blocking with customer payment cards. The criminals were still able to skim the data off these cards but quickly realized that the card data was worthless because they could not clone cards and use them in non-EMV compliant countries.

Geo-blocking, also known as regional blocking, is where payment cards are limited in their use worldwide. Regional blocking was implemented in January 2011. Belgian debit cards, by default, can only be used in Europe. Customers can inform the bank that they intend on traveling to enable use of the card outside of Europe but to date only less than 1% of Maestro customers have activated this option. In many cases, the customer can disable regional blocking through online banking. Frequent travelers can possess a payment card that does not have regional blocking.

The impact of this geo-blocking strategy is phenomenal. In 2011, Maestro fraud plummeted by 95% and the number of skimming incidents dropped by 96%. In Belgium, all Maestro (MasterCard) cards and terminals are EMV-compliant.

All POS terminals in Belgium require chip and PIN and therefore the magnetic stripe is never read. This means that there are virtually no instances of skimmer fraud on POS terminals. There have only been a few instances of petrol pump skimmers being used.

ATM Skimmer Fraud in The Netherlands

The Netherlands has a population of about 16.8 million. Skimming in The Netherlands is relatively low. Regarding losses from payment card fraud, skimmer fraud was perceived as a major risk. In 2010, skimming losses, suffered by Dutch banks, were €19.7 million. That number rose to €38.9 million in 2011 but subsequently fell back to €19.7 million in 2012. This decrease in skimmer fraud is not only attributable to the widespread use of EMV-compliant cards but to the use of geo-blocking and the installation of ATM anti-skimming devices. Additionally, no longer is the magnetic stripe being used solely in POS terminals but rather the chip and PIN are used to authenticate the user.

Regional card blocking was instituted in The Netherlands in 2012. The first major bank instituted regional blocking in June 2012 and the last major bank adopted this in March 2013. Skimmer fraud losses no longer occur in The Netherlands. The only fraud losses from skimming are from the use of cloned cards used in non-EMV countries, like the United States. There are no statistics on the impact of regional blocking for The Netherlands but indications are that skimmer fraud is on the decline.

All ATMs and POS terminals in The Netherlands are EMV since 2012. Therefore, there is no swiping of payment cards at POS retail terminals. However, there has been a shift of fraud to unmanned petrol stations, at parking machines and ATMs with poor anti-skimming technologies.

Interestingly, there are processors in The Netherlands that will not accept payment cards that do not contain an EMV chip. This is the case when trying to purchase a train ticket in The Netherlands where cards issued in the United States (without a global chip) will not be accepted. Of course, there are some retailers that do not accept credit cards.

Laying the Groundwork for ATM Skimming

The process begins with scouting out a number of ATMs in close proximity of one another and documenting the type of device that they can install. Urban areas are more conducive to criminals plying their trade because they can target more machines in a smaller geographic area on foot with great economic rewards. Very often a skimmer will be installed with an accomplice who will keep watch for law enforcement or potential witnesses.

A false front (overlay) ATM card reader is generally attached using heavy-duty double-sided adhesive tape. Sometimes a legitimate card reader is cut off an ATM to use as a prototype for an overlay card reader. This fake overlay device can be manufactured with the use of a 3D printer, which enables the user to create any plastic structure from a template. A decent 3D printer can cost

around $1,500 to $2,000. During the research, we did not encounter any European law enforcement agency seizing any 3D printers from skimmer fraud criminals.

Alternatively, a legitimate ATM card reader can be used to create rubber molds, which are later used for the creation of plastic overlays. Once the plastic has set and has been removed from the mold, it will be spray painted to match the color of the rest of the ATM. Each overlay is often numbered on the unexposed side to keep track of where each device will be installed. **Figures 9** and **10** shows an example of an ATM overlay recovered by investigators on the front and the underside with the skimmer device for recording data from the magnetic stripe on their ATM card.

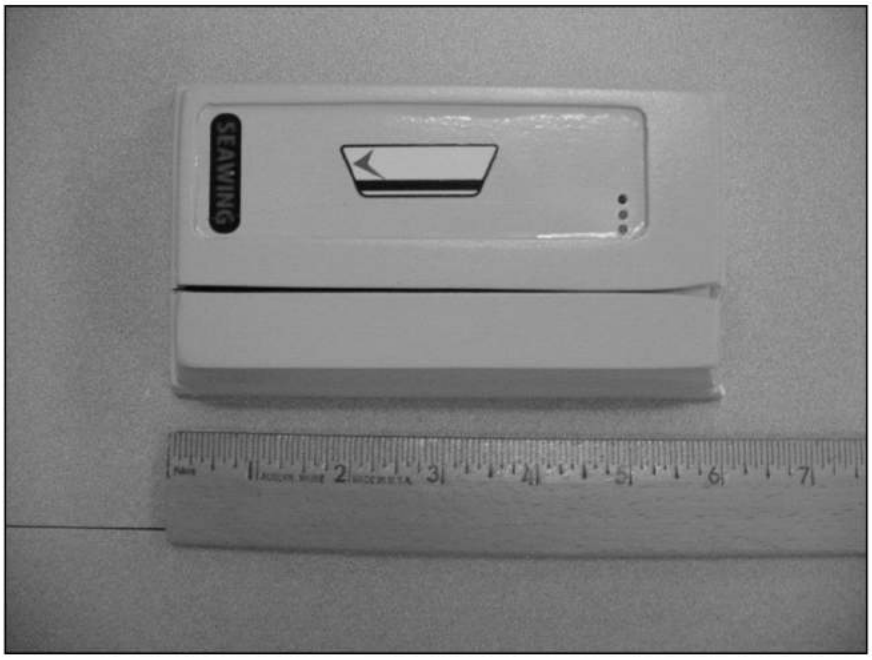

Figure 9 ATM False Door Opener Overlay

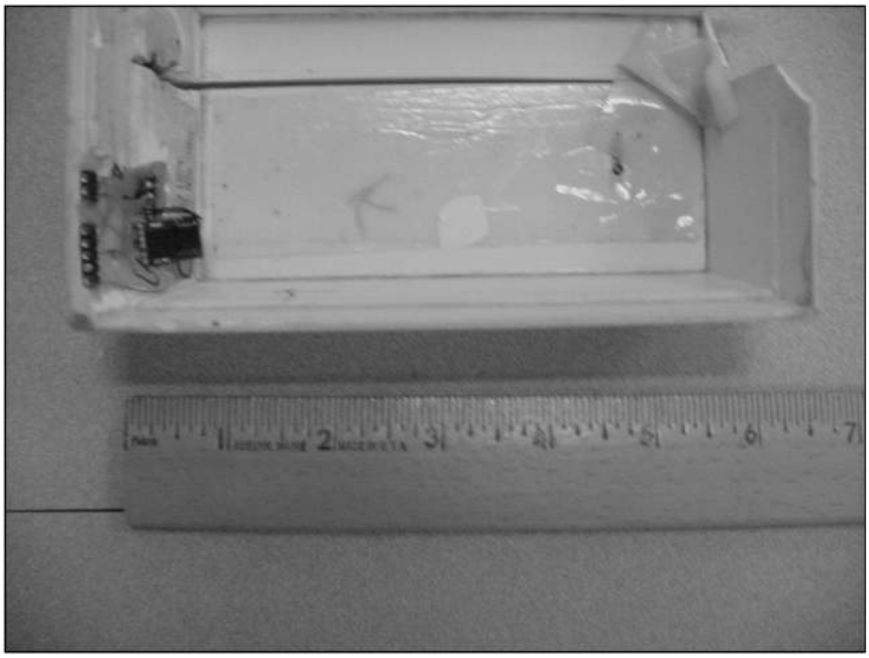

Figure 10 ATM Door Opener Skimmer on Underside of Overlay

The following skimmer was placed over the door opener at the lobby to an HSBC ATM. The legitimate door opener is at the top of **Figure 11**, while the skimming device is at the bottom of the image.

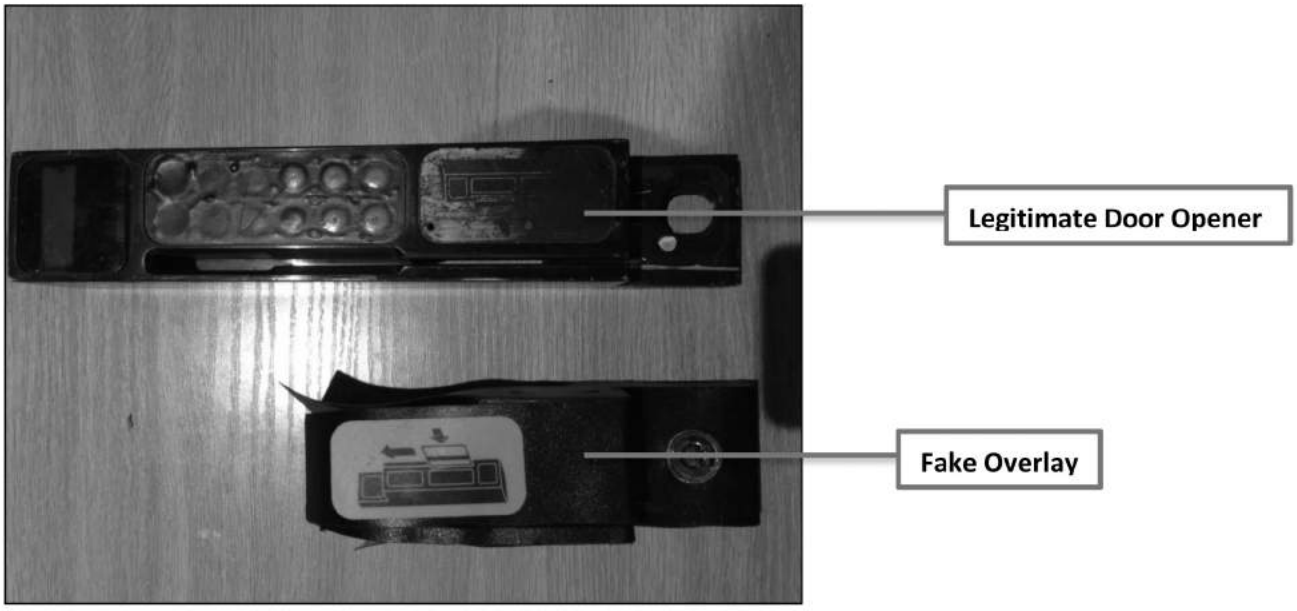

Figure 11 ATM Door Opener Skimmer

Figure 12 shows the skimmer placed over the legitimate door opener.

Figure 12 ATM Door Opener Skimmer Placed Over Legitimate Door Opener

Skimmers found on door openers have become so problematic that some banks have decided to deactivate these card slots. This is the case in Germany for example.

The criminal will also install a pinhole camera, close to the keypad, to record the user PINs. These cameras can be hidden by leaflet holders, housed in smoke detectors or masked by other innocuous-looking devices. Very often though, the camera is installed in the plate above the PIN pad. In **Figure 13** you can view the wireless camera mounted on a plate that will be installed above the PIN pad on the ATM. The black box, located at the top of the image, is used for receiving video of customers entering their PIN on the keypad.

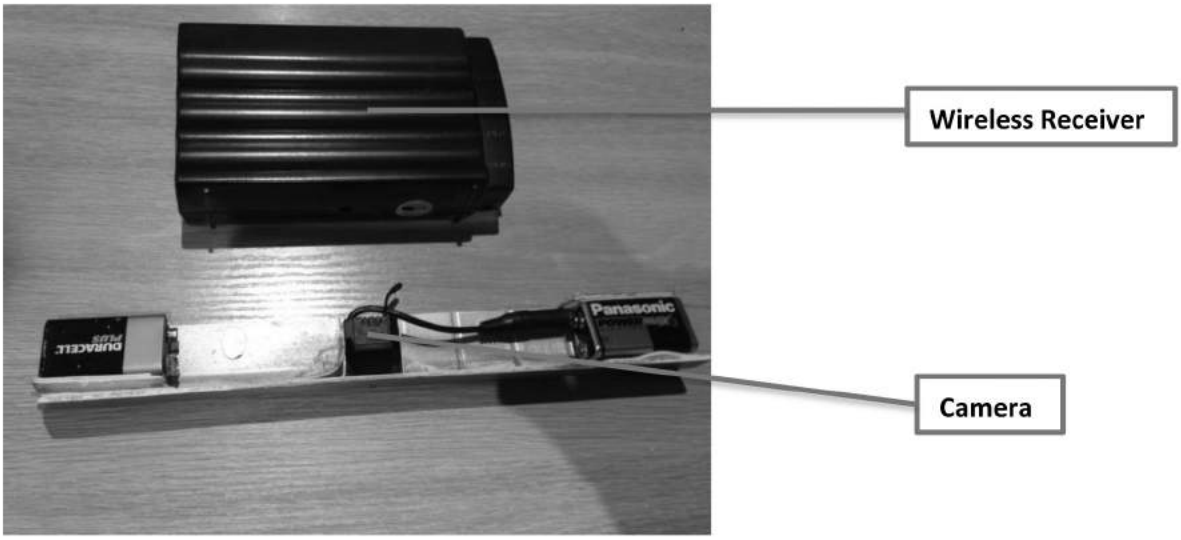

Figure 13 Wireless Transmitting Camera & Receiver

These cameras can be purchased from spy stores or online sites like Amazon.com. These cameras are sometimes powered by cellphone batteries, which are relatively small but have a long-lasting charge. In one case, the camera from a Nokia cellphone was used and it was attached to a USB to collect the video.

It is important for the criminal to be able to synchronize the PIN entries recorded by the camera with the data that is being recorded by the skimming device. In **Figure 14** we can actually view the notes found in the possession of a suspect who was arrested on suspicion of skimmer fraud. Here is an explanation of what the notes mean:

Column 1 – Skimmer Record Number: the skimmer device stores each magnetic stripe as a separate sequentially-numbered record.

Column 2 – PIN: these are the PIN numbers recorded by the video. The term "RAT" refers to the criminal's inability to recover the PIN because the customer covered the keypad with their hand.

Column 3 – Start Time: this is the time on the video that the customer starts to use the ATM.

Column 4 – End Time: this is the time on the video that the customer ends her use the ATM.

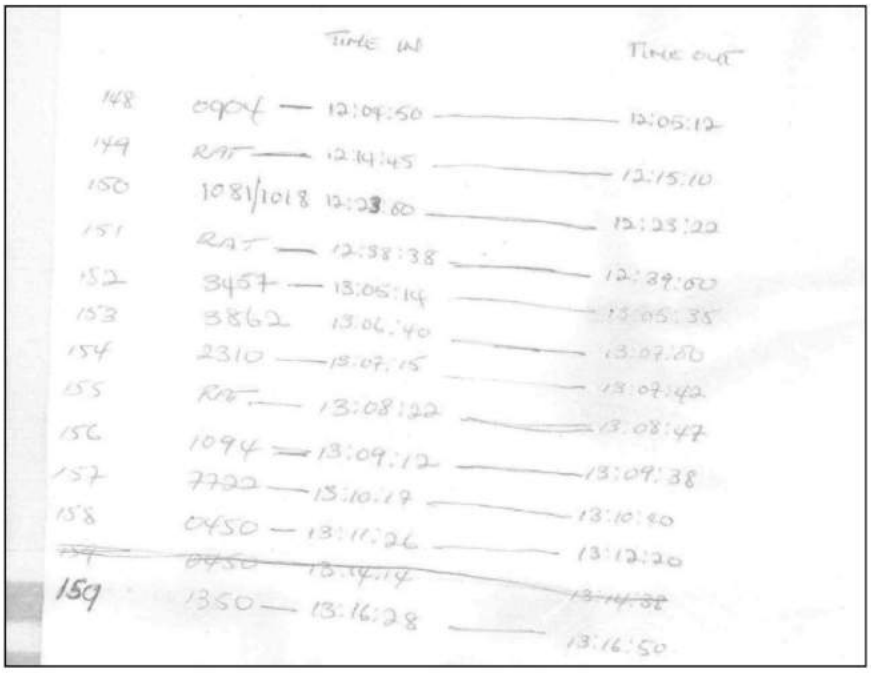

Figure 14 Criminal Skimmer Notes

Alternatively, an overlay keyboard can be placed on top of the existing PIN keyboard on an ATM to record the user PIN. It should be noted that overlay keypads are not that prevalent because the keypad needs to be molded to fit each model of ATM and the cost is higher than using a pinhole camera; the price of pinhole cameras has dramatically decreased in recent times. The data downloaded from the cameras and skimmer devices are often password protected or encrypted. These devices are not just encrypted to thwart efforts by law enforcement, who seek to access the

credit card data, but are also used by gang leaders to prevent their accomplices from taking the skimmed data for their own use.

More advanced ATM skimmers can actually provide the criminal with SMS (Short Message Service) or Bluetooth notification of successful magnetic stripe captures.

Once the data from the ATM, debit or credit cards is downloaded, along with the corresponding PINs, replica cards can be manufactured by the criminals and used to withdraw funds.

Anatomy of a Skimmer

Skimmers have existed for many years now and they have advanced quite considerably over time. They have become smaller and have more memory. In fact, when a skimmer is found the memory is usually not fully used because of their large memory capacity. The quality of data on these devices has also improved over time, which is exemplified by fewer read errors. These skimmers are often password protected and use advanced encryption protocols. **Figure 15** shows an example of a more advanced skimmer that was recently seized by police. These skimmers have been used by criminals operating in Spain and in the U.K.

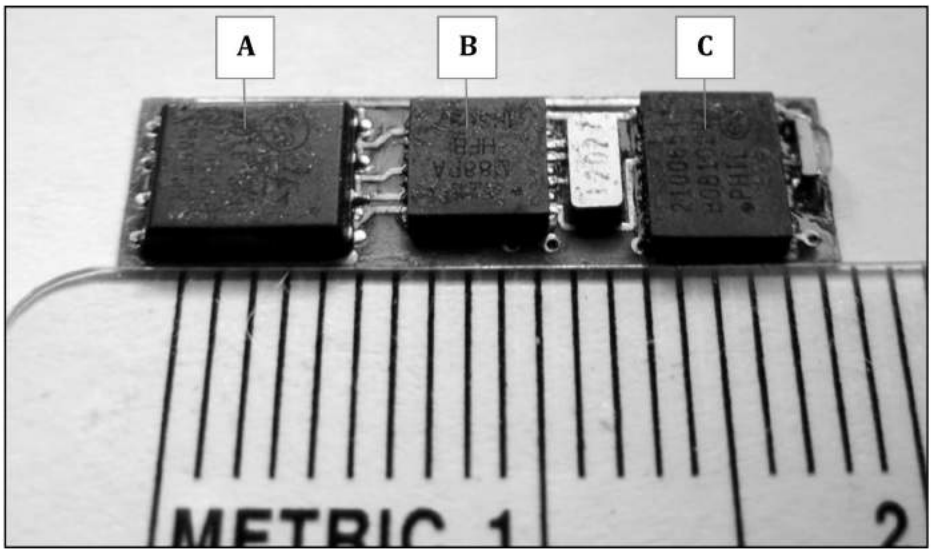

Figure 15 Skimmer

A – Serial EEPROM
B – Microcontroller
C – F2F Converter: Magtek 21006516 (Magnetic Head to Digital Data Decoder)

The programmable microcontroller is the brains of the skimmer and this is where the encryption, utilized by the criminal, resides. The serial EEPROM is the memory where the card skimmed card data is stored. The magnetic head to digital data decoder is where the data from the magnetic stripe is read before it is processed.

Magnetic Stripe

The goal of skimmer fraud criminals is to steal the data stored on the magnetic stripe, which is located on the back of the payment card. The data is stored in plaintext, which means that the criminal does not need to decrypt the data stored on the back. You will notice from the explanation below that the user PIN is not stored on the payment card and therefore the criminal will need to obtain that number for ATM cards using a pinhole camera or through other means. Gasoline (petrol) stations and other retailers in the United States will often verify the legitimacy of the card user by requiring that the user provide a zip code for the address associated with the card. This is because the zip code is not stored in the magnetic stripe.

Track 1 and Track 2 data standards are defined under ISO/IEC 7813:2006.[35] Track 3 data standards are defined under ISO/IEC 4909:2006.[36]

There are usually three tracks of data stored on the magnetic stripe.

Track 1

Track 1 supports a higher bit density and is the only track that supports alphabetical characters. Therefore, only Track 1 will contain the name of the cardholder. The card issuer may use a proprietary format for the order of characters. The following is the layout of data on Track 1:

SS	FC	PAN	FS	Name	FS	ED	SC	DD	ES	LRC

SS – Start Sentinel (usually "%")

FC – Format Code (1 character)

PAN – Primary Account Number (maximum of 19 characters and is often the credit card number)

FS – Field Separator (usually "^")

Name – 2 to 26 (alpha-numeric characters)

FS – Field Separator (usually "^")

ED – Expiration Date (YYMM)

SC – Service Code (three characters)

DD – Discretionary Data (may include a PIN Verification Key Indicator (PVKI), PIN Verification Value (PVV), Card Verification Value (CVV) or Card Verification Code (CVC))

ES – End Sentinel (usually "?")

LRC – Longitudinal Redundancy Check (one character)

[35] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=43317
[36] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=43309

Track 2

The format of Track 2 data was developed by the American Banking Association (ABA). Track 2 can hold up to 16 characters, including numbers 0-9 and the following six characters:

: ; < = > ?

The following is the layout of data on Track 2:

SS	PAN	S	ED	SC	DD	ES	LRC

SS – Start Sentinel (usually ";")

PAN – Primary Account Number (maximum of 19 characters and is often the credit card number)

S – Separator (usually "=")

ED – Expiration Date (YYMM)

SC – Service Code (three digits)

DD – Discretionary Data (may include a PIN Verification Key Indicator (PVKI), PIN Verification Value (PVV), Card Verification Value (CVV) or Card Verification Code (CVC))

ES – End Sentinel (usually "?")

LRC – Longitudinal Redundancy Check (one character)

The Service Code will provide information about when the PIN is required and define whether the card has an embedded global EMV chip (IC).

Track 3

Track 3 is unused by most financial networks.

Interestingly, some criminals will actually copy skimmed data onto their own personal credit card. Using a microscope, an investigator can view the recorded data overwritten onto existing magnetic stripe data. The payment card will still work.

Equipment Used for ATM Skimmers & Card Reproduction

- Plastic resin, rubber mold and paint (used to make and add color to an ATM overlay);
- 3D printer (can be used to make an overlay instead of using an overlay mold);
- Heavy-duty double sided tape (used to attach a resin overlay);
- Pinhole camera and battery (used to record user PIN);
- Skimming device (records data from magnetic stripe on card);
- Computer (used to download card user data from skimmer);
- Black card stock (used to create cloned cards);
- Magnetic stripe reader-writer (used to add data downloaded from skimmer to blank card); and

- Card printer (optional - used for adding artwork to blank plastic card).

Sometimes these criminals have been arrested in possession of color charts relating to different colors found on ATMs. In the U.K., possession of these ATM color charts is an offense.

VII. Criminal Profiles

Criminals involved in skimmer fraud will generally work in small organized groups rather than as individuals. Thus, they are more effective in scouting out a larger number of potential targets. As a group, a number of targets can be hit in quick succession before bank officials or law enforcement are alerted. These organized criminals operate globally and are highly coordinated. For example, the criminals will often travel from Eastern Europe to Western European countries with skimmers, skim cards in Western Europe and are then arrested in countries like Ghana, Costa Rica or the United States. Therefore, the coordination of law enforcement agencies worldwide is critical.

According to CELT Ltd., from 1994 to May 2003, in the U.K. and other parts of Europe, skimming was primarily limited to petrol (gasoline) stations and restaurants and the criminals were often Sri Lankan (Tamil). After May 2003, it appears that organized criminals from Romania and Bulgaria took over this criminal activity.

Skimmer thieves of all nationalities are arrested in the United States and around the world. Nevertheless, it appears that a significant number of these criminals arrested are Eastern European and very often are from Romania or Bulgaria. We can even go further and identify certain cities where these criminals come from. For example, many of those arrested have come from Craiova in Romania. The theory that many of these criminals come from the same areas in Romania and Bulgaria seems less circumstantial when analyzing reports of arrests in Europe, Africa and Asia. Moreover, there are a number of reports documenting the Romanian Directorate for Investigating Organized Crime and Terrorism (DIICOT) infiltrating skimmer fraud rings and manufacturing operations in Dolj County, including Craiova City and Bucharest. According to law enforcement, some of those arrested in the United States are unemployed electricians.

Over the years, skimmers have become smaller and more sophisticated in terms of power, memory, communication and encryption. These technical advances have prompted some investigators to believe that skimmer technologies are probably being developed by electronic engineering and computer science students at universities in Romania and Bulgaria. These countries possess an excellent educational system. It must be emphasized that this hypothesis could not be validated but investigators interviewed from a number of countries noted their belief that university students were working on skimmer technologies. Some of those arrested have been unemployed electronic engineers. Law enforcement agencies in Europe have indicated that the Bulgarian gangs are better organized and their leaders pay their members more money than their Romanian counterparts.

Skimmers are not only manufactured in Romania but also in Bulgaria. The criminals are very creative with the methods they use to export these devices across international borders. In February 2013, the Sofia News Agency reported that Bulgarian customs officials seized ATM skimmer device parts at Kalotina, from a Bulgarian national traveling on a bus from Bulgaria to Germany. The skimmer parts were hidden in croissants, a reader and batteries were hidden in a

medicine box and other parts of suspect's luggage.[37] Law enforcement has found skimmers printed circuit boards (PCB) smuggled in electronics, including DVD players. Hiding these skimmer PCBs in electronics make them more difficult to detect.

According to Europol, law enforcement in Bulgaria has reported that criminals and gangs that have traditionally been known for involvement in drug trafficking, counterfeiting, theft and vehicle crime have become more involved in payment card fraud schemes, which are perceived to be lower risk activities and carry lower penalties.[38]

A number of organized crime groups in China and Southeast Asia have been cloning payment cards and then sending "mules", using forged travel documents, to Western Europe to fraudulently purchase luxury goods, which are then sent back to Asia.[39]

Skimmers to Fund Terrorism

Although skimmer fraud has been primarily associated with Eastern European countries, other factions have been involved with this fraud because it is a fast way to steal money. Brahim Benmerzouga and Baghdad Meziane were two Algerians, connected to al-Qaeda, who were arrested in the U.K. on suspicion of raising money for terrorist activities.[40] Police found skimming devices, stolen credit card information and other credit card paraphernalia in Benmerzouga's car. Ultimately, both suspects were found guilty in 2003 and sentenced to 11 years in prison.

The Armed Islamic Group of Algeria, known in France as the GIA, has used card skimming to fund their terrorist activities. Reda Hassaine, an informer for British and French intelligence, detailed how some extremists, associated with the Finsbury Park mosque in London, were recruiting people working at restaurants, petrol stations and hotels to use skimmers.[41]

On March 11, 2004, ten explosions were detonated on four commuter trains in Madrid, Spain. These horrific bombings resulted in the deaths of 191 people and injured more than 1,800. One of the deceased was, according to Spanish police, the ringleader - Serhane ben Abdelmajid Fakhet, who was Tunisian. Some have speculated that the Moroccan Islamic Combatant Group (GICM) was responsible for the bombings. Informal conversations have revealed that skimmer fraud paraphernalia was seized from the homes of the suspects that were arrested.

Major ATM Skimmer Fraud Schemes

The following is a snapshot of major POS skimmer fraud schemes in recent years:

---

[37] http://www.novinite.com/view_news.php?id=147460
[38] "EU Organised Crime Threat Assessment", OCTA 2011, Europol.
[39] "EU Organised Crime Threat Assessment", OCTA 2011, Europol.
[40] http://www.telegraph.co.uk/news/uknews/1426340/Quiet-lives-hid-a-quest-to-recruit-for-global-jihad.html
[41] http://www.historycommons.org/timeline.jsp?complete_911_timeline_possible_moles_or_informants=complete_911_timeline_abu_hamza_al_masri&timeline=complete_911_timeline

$45 million – May 2013, thousands of ATM machines were hit by criminals simultaneously around the world;[42]

$3.3 million – January 2013, Romanian suspect, Mihai Vasile Bandura, was accused of skimming the debit cards of 200 Bank of Prairie du Sac customers;[43]

$1 million – January 2013, Romanian suspects, Constantin Ginga and Marius Gheorghe Cotiga, were charged with theft, conspiracy to commit theft, financial facilitation and credit card fraud, in New Jersey. They were suspected of installing skimming devices at TD Bank and Citibank ATMs;[44]

$1.5 million – January 2012, Romanian suspect, Laurentiu Iulian Bulat, was arrested while trying to install high-tech skimmers on HSBC ATMs in New York City;[45]

€50 million – July 2011, more than 200 police officers conducted simultaneous arrests in Bulgaria, Italy, Spain, Poland and the United States. The primary focus was in Bulgaria, where 47 suspects were arrested by 150 police officers. This organized crime group was suspected of defrauding thousands of EU citizens and cloning over 15,000 payment cards; and

$1 million – September 2010, Bulgarian suspect, Radostin Paralingov, was arrested in Las Vegas for using ATM skimmers in New York City to defraud customers of two banks.[46]

Automated Teller Machine Security – A Global Perspective

Latin America is a growing market in terms of new ATMs, with a majority of new machines being installed in Brazil.[47] The ATM market in Asia is growing rapidly, with much of the expansion being attributed to growth in the Chinese market.[48] It is estimated that as of June 30, 2012, there were 409,830 ATMs in Europe with 70% of those deployed in U.K., Spain, Germany, France and Italy (288,300), according to EAST.[49]

VIII. European Security Standards (EMV)

Security standards with European credit, debit and ATM cards differ from standards in the United States. In Europe there are EMV (Europay, MasterCard and Visa) cards, which include a chip. It is an open standard for smartcard payment processing, which was built for financial and retailing institutions globally. According to EMVCo, the official information source for the EMV standards body, there were 1.55 billion EMV-compliant chip-based payment cards being used worldwide, as

[42] http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?_r=0

[43] http://www.wiscnews.com/news/local/article_74a0527e-6b66-11e2-95a0-001a4bcf887a.html?comment_form=true

[44] http://www.nj.com/bergen/index.ssf/2013/01/romanian_immigrants_charged_with_running_1_million_atm_skimming_scheme.html

[45] http://www.nypost.com/p/news/local/manhattan/skim_scam_man_YVv85DNKwBUGoPevYLzJPK

[46] http://www.fbi.gov/newyork/press-releases/2010/nyfo092310a.htm

[47] Retail Banking Research

[48] Retail Banking Research

[49] "European ATM Crime", EAST, 2012.

of Q2, 2012.[50] Also according to EMVCo, there are 22 million point-of-sale terminals that are EMV compliant.

The chip in an EMV card is an integrated circuit (IC) and is embedded in the card for added security. The chip enables a card to be used with EMV-enabled devices, including ATM and point-of-sale (POS) terminals. EMV is a two-factor authentication protocol, with the chip and user PIN authenticating the consumer. Nevertheless, EMV cards can be used globally on devices that do not recognize the IC chip. This is important because cards stolen in Europe, or cards reproduced from legitimate European cards, are very often brought to the United States by criminals. According to Europol, 80% of fraud outside the EU, using EU payment cards, occurs in the United States, which translates into $1 billion in losses. According to the European ATM Security Team, EMV adoption in Europe was 98%, in Russia 75% and in Canada 65% in 2011. By Q2 2012, EAST estimates that 99.2% of ATMs are EMV-compliant, which represents a significant increase from 2005 when only 52% of ATMs were compliant.[51]

There is a strong argument for introducing this international standard and EMV will be implemented in the United States. EMV was recently introduced in Canada. In the U.K., EMV was introduced in 2002. The previous year, card fraud cost the U.K. £160.4 million. By 2011, that number had fallen to £36.1 million. Nevertheless, ATM skimmer fraud remains an issue in Europe and, according to EAST, resulted in €111 million in losses in the first six months of 2011. However, the same study reported that card skimmer losses are on the decline.[52] A more recent report from EAST shows skimmer fraud to be still a significant problem in Europe, with reported losses of approximately €128 million in the first half of 2012.[53] However, this notable increase appears to be associated with losses by international issuer losses.

It should be noted that EMV is not a perfect solution. A recent study at the University of Cambridge, U.K., demonstrated how EMV cards can be subject to "pre-play" attacks.[54] This research identifies a vulnerability associated with the random, unpredictable number called a nonce, which can be predicted due to the poor execution practices of some EMV implementers.

EMV in the United States

There has been no mandate for the introduction of EMV in the United States, unlike the introduction of EMV in the U.K., Canada and Mexico. Nevertheless, it will be introduced with a timeline of 2016/2017 – prompted by a shift in liability. It has been announced that once EMV is fully implemented in the United States, non-EMV compliant banks and retailers will be forced to absorb any losses associated with fraudulent transactions.[55]

---

[50] www.envco.com
[51] "European ATM Crime", EAST, 2012.
[52] http://www.diebold.com/atmsecurity/files/DBD_ATMFraud_WP.pdf
[53] "European ATM Crime", EAST, 2012.
[54] Bond, Mike, et al, "Chip and Skim: cloning EMV cards with the pre-play attack", University of Cambridge, September 2012.
[55] www.atmmarketplace.com

Making ATMs EMV-compliant will occur by either purchasing an upgrade kit or by trading in machines for credit towards new ATMs. Many acquirers and ATM manufacturers believe that the timeline for converting to EMV-compliant ATMs and point-of-sale terminals is unrealistic.[56] Nevertheless, it is important to understand that acquirers are procrastinating with implementing EMV-compliant terminals, according to a recent report.[57]

In April 1, 2013, MasterCard, Visa, American Express and Discover expected that U.S. networks and processors should be able to process EMV transactions. These processors were supposed to certify that they can handle these transactions by April but given the scope of this initiative its successful implementation by April 2013 has been problematic. Although there is no penalty for non-compliance, in some cases an issuer may hold a bank liable for any losses. The cost for upgrading ATMs and point-of-sale terminals is expensive and time-consuming and the timetable provided appears to be causing tremendous concern. A recent survey, conducted at the end of 2012, by the ATM Industry Association and Kahuna ATM Solutions, indicated that implementation of EMV and meeting issuer deadlines was the greatest concern for IADs (Independent ATM Deployer).[58]

In September 2012, MasterCard announced the expansion of EMV-compliance to include the ATM channel.[59] If a Maestro EMV card is used at a non-EMV-compliant ATM in the United States and the transaction is later deemed to be fraudulent then the loss can be charged back to the ATM proprietor. Issuers have traditionally bore fraudulent losses so this is a dramatic shift of responsibility.

In August 2011, Visa announced their decision to mandate payment processors to migrate to EMV chip technology.[60] Visa has however offered concessions to these processors by waiving Payment Card Industry Data Security Standard (PCI DSS) compliance validation requirements. Like MasterCard, Visa is also shifting liability with EMV compliance at U.S. ATMs. By April 1, 2015, all third-party ATM acquirers in the United States must support EMV chip data and liability will shift effective October 1, 2017.[61]

American Express has joined other card issuers in requiring processors to be EMV-compliant by April 2013.[62] In October 2013 processors received relief from PCI DSS reporting requirements where 75% of a merchant's POS transactions are processed through American Express EMV chip-based contact and contactless transactions. Effective October 2015, American Express will introduce a policy called Fraud Liability Shift (FLS), which is a liability shift. The liability shift will be implemented for gasoline vendors in October 2017.

---

[56] http://www.atmmarketplace.com/article/215895/The-daunting-logistics-of-US-EMV?utm_source=NetWorld%20Alliance&utm_medium=email&utm_campaign=EMNAAMC07102013
[57] http://www.atmmarketplace.com/article/215895/The-daunting-logistics-of-US-EMV?utm_source=NetWorld%20Alliance&utm_medium=email&utm_campaign=EMNAAMC07102013
[58] http://www.atmmarketplace.com/article/208695/Study-reveals-major-concerns-of-ATM-independents
[59] http://newsroom.mastercard.com/press-releases/mastercard-extends-u-s-emv-migration-roadmap-to-atm-channel/
[60] http://usa.visa.com/download/merchants/bulletin-us-acquirer-mandate-080911.pdf
[61] http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1780934&highlight
[62] http://about.americanexpress.com/news/pr/2012/emv_roadmap.aspx

Discover is also implementing an EMV mandate in the United States, Canada and Mexico.[63] Discover processed its first EMV card transactions in the United States in January 2012.

EMV Implementation in Other Countries

Visa has outlined a timetable for shifting responsibility for EMV compliance to ATM acquirers in other countries worldwide:

- Beginning April 1, 2013, liability shifted in Australia and New Zealand;[64]
- Beginning October 1, 2015, liability will shift in Asia Pacific, excluding China, India, Japan, and Thailand; and
- Beginning October 1, 2015, liability will shift in China, India, Japan and Thailand.

IX. The Future of ATM Transactions

Biometric Security

In a number of countries, including Brazil and Japan, biometrics are used to authentic a user. The biometric used can include fingerprint, palm print or iris. The use of biometric authentication is controversial because if your biometric is stolen then it can never be replaced – unlike a payment account number.

Brazil's second largest bank, Banco Bradesco, operates 33,000 ATMs and 90% of these machines are palm-vein enabled. Fujitsu provides this biometric authentication solution known as PalmSecure technology.[65] Banco Bradesco has 10 million customers.

Contactless Cards

Some countries are working on using cards that are merely moved over a certain part of the ATM rather than being swiped and then a PIN is entered for larger withdrawal requests. As previously mentioned, Visa's *payWave*, MasterCard's *PayPass* and *girocard* are all contactless card protocols. Contactless cards rely on radio frequency identification (RFID) technology for communication with a terminal.

Smartphone Withdrawals

Near Field Communication (NFC) is found in some smartphones and tablets, like the Samsung Galaxy III S. This communication protocol, which is already being used for business transactions, would utilize a smartphone for ATM transactions instead of using an ATM card. Visa has already declared its support of NFC-based mobile payments. Visa believes it is prudent to incentivize payment processors to not only support EMV chips but also NFC tags.[66] Visa believes that encouraging processors to support both EMV and NFC will promote innovation in mobile payment technologies while significantly improving security.

---

[63] http://discovernetworknews.com/stories/discover-implements-emv-mandate-for-u-s-canada-and-mexico/
[64] http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1780934&highlight
[65] http://www.fujitsu.com/us/services/biometrics/palm-vein/banking.html
[66] http://usa.visa.com/download/merchants/bulletin-us-acquirer-mandate-080911.pdf

In the U.K., Royal Bank of Scotland (RBS) and NatWest customers can use banking applications (apps) on their smartphones to withdraw cash without a card. The user simply makes a request, using the banking app, to withdraw up to £300. A six-digit code is then generated, which the customer can then use at an RBS, NatWest or Tesco-branded ATM.[67]

NCR Corporation recently announced an ATM mobile application for iPhone and Android smartphones called NCR Mobile Cash Withdrawal.[68] This technology also does not require a card or PIN but rather authenticates the user through his device. The customer can request a cash withdrawal and is then provided with a 2D barcode, which can then be scanned at an NCR ATM.

Bitcoin ATMs

The first Bitcoin ATM was installed in a Vancouver coffee shop in 2013 and more of these ATMs are likely to be unveiled in 2014. Robocoin Technologies, which manufactures Bitcoin ATMs, appears likely to install another one of these machines in Hong Kong.[69] These ATMs use biometric authentication rather than a payment card to transact Bitcoin. It will be very interesting to see how many of these Bitcoin ATMs will begin appearing in 2014.

Prevention of ATM Skimming

Some of the future technologies previously discussed do mitigate many of the risks associated with ATM skimmers. However, there is a need to protect ATMs acquirers that have not yet introduced new anti-skimming technologies. Anti-skimming devices have been installed by some financial institutions. However, there have been reports of some criminals being able to circumvent these new devices; Vitalli Pascari was arrested by Gardaí (Irish police) in November 2010 and was found in possession of AIB ATM parts that were claimed to be tamper-proof.[70] Additionally, regional blocking does prevent skimmer fraud. The introduction of EMV in the United States and other countries should lead to a dramatic reduction in skimmer fraud.

The following represents a series of actions that can be taken to prevent – or reduce the risk of – skimmer fraud:

Customer Protection

1. Cover the Keypad

Customers should use one hand to cover the keypad while entering their PIN.

2. Customer Alert System

Customers should be provided with information about identifying potential skimmers and how to alert authorities.

3. Situational Awareness

Customers should be aware of their surroundings and be careful of criminals shoulder surfing.

---

[67] http://www.bbc.co.uk/news/business-18409560
[68] http://www.ncr.com/newsroom/resources/mobile-cash-withdrawal-news
[69] http://www.zdnet.com/bitcoin-atm-to-dispense-in-hong-kong-but-not-taiwan-7000024868/
[70] http://www.limerickpost.ie/index.php/navigation-mainmenu-30/local-news/4193-5-year-sentence-for-running-global-atm-skimming-operation-from-limerick-suburbs.html

4. Monitoring

All bank customers should regularly monitor their accounts online, financial statements and credit reports to check for fraudulent transactions. Ensure that your financial institutions have all of your up-to-date contact information, including your current mobile telephone number.

ATM Protection

1. Lighting

Ensure that ATMs have ample lighting and ensure good visibility for passers-by.

2. Closed Circuit Television (CCTV)

The use of cameras to record activity at ATMs is important but maintaining adequate memory to store video for an extended period of time is a necessity.

3. Overlay Installation Alert Technology

There are technologies being used by banks today that will alert institutions when overlay devices are being fitted by criminals.

4. Regular Inspection

A bank can have its employees regularly inspect their ATMs for loose card readers. Additionally, there are cards available that look like a credit card but are thicker. If a skimmer has been added to the motorized card slot then the skimmer detection card will become jammed in the card slot. If the card slides in unabated then it is unlikely that a skimmer has not been added to the machine.

X. Gasoline Pump Skimmers

Gas pump skimmers are not nearly as prolific as ATM skimmers or even handheld skimmers. Nevertheless, there are sporadic incidences of gas pump skimmers. One notable scam involving these skimmers was uncovered in 2013 when the New York County District Attorney indicted four suspects on charges relating to their use of skimming devices at RaceTrac and RaceWay gas stations in Texas, Tennessee, and Georgia.[71] It is estimated that thieves had stolen $2.1 million from stolen credit and debit cards.

XI. Ticket Machine Skimmers

Skimming devices have been found at ticket vending machines in the United States, Peru, Dominican Republic and, more recently, in Ireland. A "throat skimmer" is used in conjunction with small camera. The Garda Bureau of Fraud Investigation recently discovered these skimming devices at railway stations in Dublin.[72] Skimmer fraud scams in Ireland are believed to have been organized by Romanian crime boss Vasile Martin.[73]

---

[71] http://techcrunch.com/2014/01/23/four-indicted-for-installing-undetectable-card-skimmers-inside-gas-pumps/

[72] http://www.irishtimes.com/newspaper/breaking/2012/1126/breaking12.html

[73] http://www.independent.ie/irish-news/courts/skimmers-who-hit-mcaleese-for-5000-are-jailed-26685371.html

XII. Point-Of-Sale Terminal Skimmers

Point-of-sale (POS) skimmers are problematic worldwide but do not appear to be as much of an issue in the European Union as they are in United States. This is probably because many POS terminals in the EU read the magnetic stripe and chip on an EMV card and implanting a skimmer is more involved in Europe than in the United States. **Figure 16** shows a typical POS terminal that is used in Europe.

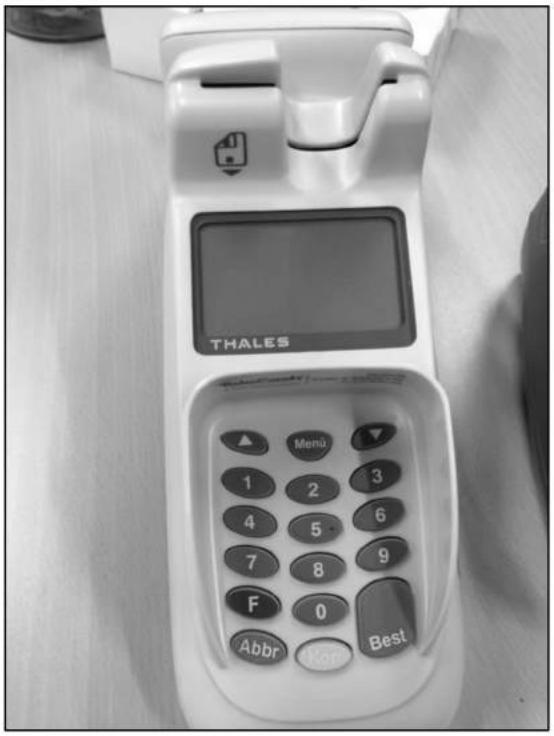

Figure 16 Thales POS Terminal

Figure 17 Thales POS Terminal with Cover Removed

When the cover is removed from the terminal, the machine still appears to be undefiled but upon closer inspection we can ascertain that the machine has been altered by criminals, as shown in **Figure 18**.

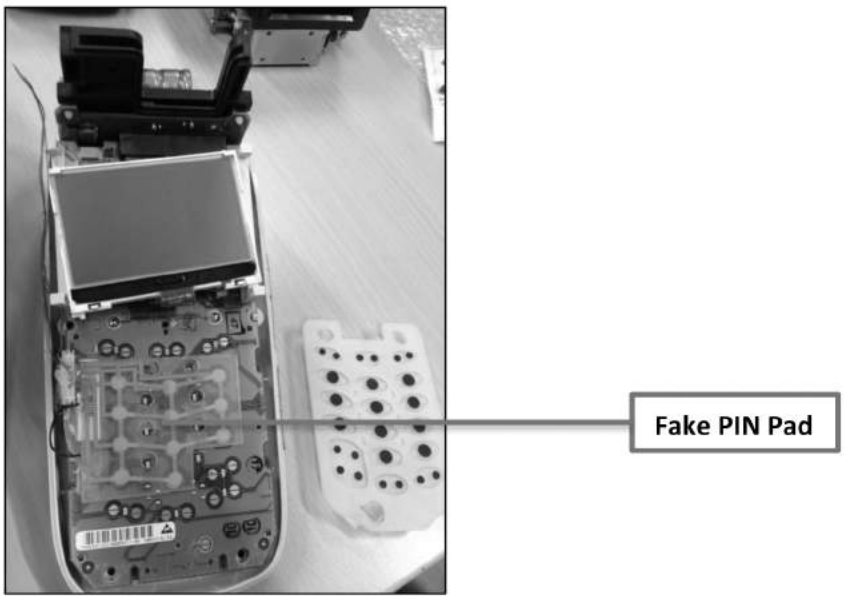

Figure 18 False PIN Pad Added to Terminal

Once the legitimate PIN pad is removed from the terminal, we can see that criminals have added a false PIN pad to record the PIN number entered by the customer. A skimmer has also been added by the criminal to skim the card data from the magnetic stripe as the card is inserted into the terminal's card dip reader.

Major POS Skimmer Fraud Schemes

The following is a snapshot of major POS skimmer fraud schemes in recent years:

$4.5 million – October 2009, POS skimmers were found at McDonald's restaurants and impacted 3,500 customers in Perth, Australia.

$1 million+ – May 2011, POS skimmers were found at 90 Michael's Stores across 20 states in the United States. 720 PIN pads are replaced at 964 stores.

$1 million+ – November 2011, POS skimmers were found at 19 Lucky Supermarkets and one Save Mart. The company replaced POS card readers at 234 of its locations.

POS Protection for the Acquirer

1. Constant Surveillance of Terminals

Ensure that POS terminals are under constant surveillance, through the use of closed-circuit television cameras, which allow security personnel to observe whether a criminal has attempted to install skimmers. Terminals should remain under the watchful eye of employees. Therefore, where possible, the cashier must never leave sight of the terminal or at least have another employee watch over the terminal when the cashier needs to be excused.

2. Protection of Supply Chain
Ensure that receiving and distribution centers maintain tight security over shipments of POS terminals.

3. POS Security
There are POS terminals that possess anti-skimming devices, i.e. a terminal will be disabled if a criminal attempts to tamper with the terminal. Consider using these devices to prevent skimmer fraud.

4. Verification of Consumer
Unfortunately very few POS acquirers require their employees to verify the legitimacy of the cardholder. Requiring that a consumer verify their identity through the presentation of a driver's license takes very little time but can reduce fraud dramatically.

5. Use of EMV Terminals
Since the EMV chip cannot be cloned, the elimination of swipe terminals and the authentication of a legitimate card through its IC (chip) will reduce POS skimmer fraud significantly.

XIII. Handheld Skimmers

When the question is posed, "Which is safer – using your credit card online or in a restaurant?" the answer invariably is "in a restaurant". That answer is not entirely true however. Online retailers very often do not even store credit card information but instead forward customer card details directly to card processors in an encrypted format. However, there have been numerous incidents involving the use of handheld skimmers at various vendors and in particular at restaurants.

Although no empirical evidence is available, it appears that handheld skimming is not prevalent in the European Union, unlike the United States.

Handheld Skimmer Device Technology

The images below illustrate just how small handheld devices are. These devices are generally powered by a battery. They can be either purchased online or made at home with components from a local electronics store. Originally, handheld skimmers were larger devices, as shown in **Figure 19**.

Figure 19 SMAG DC Handheld Skimmer

Over the years they became smaller, as shown in **Figure 20** below.

Figure 20 PMR102 (A.K.A. TA 90) Handheld Skimmer

Recently, much smaller handheld skimmers have been found in the possession of criminals, as shown in **Figures 21** and **22** below.

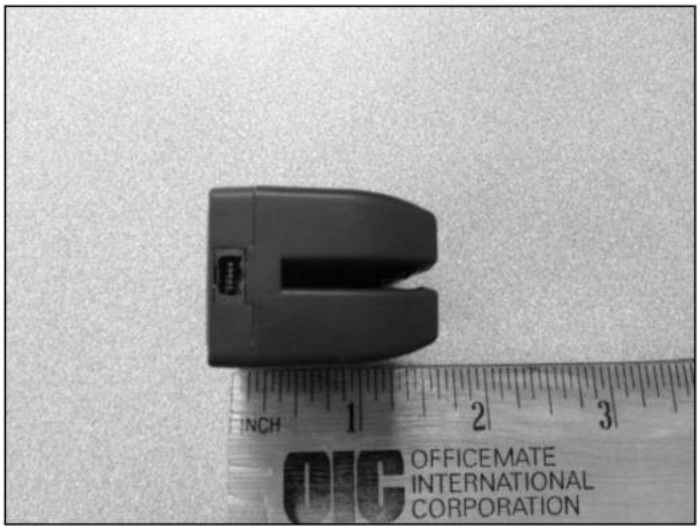

Figure 21 Side View of Handheld Skimmer

Figure 22 Top View of Handheld Skimmer

Handheld Skimmer Fraud Organization

Handheld skimmer fraud typically involves a number of people in specialized roles. A number of criminal field operatives will use the skimmer to skim the data from customer credit cards. A tech-savvy criminal will then download the skimmed card information from the skimming devices. The group would also have a supply of blank plastic cards, complete with a customizable magnetic stripe. Blank cards can be bought at a number of different retailers, like alibaba.com for example. A magnetic stripe encoder machine would also be used to write the stolen data to the magnetic stripe on these new cards. Websites like magencoders.com sell these devices. A credit card printer would also be owned by one of these groups to add the necessary artwork to the blank cards. Once the artwork had been added to the blank cards and their magnetic stripes encoded, the cards would be ready to be embossed. Embossing machines can be purchased from Websites, like saferwholesale.com. The customer name, card number and expiration date would be embossed

onto the fake cards. Once this final process has been completed, a group of "shoppers" is assembled. The shoppers will be provided with phony cards and fake drivers licenses. The shoppers will be sent out to purchase high-end luxury goods, like iPhones or Macbooks and these items can be later sold on the black market or on sites like ebay.com or craigslist.com.

Equipment Used for Credit Card Reproduction

- Handheld skimming device (records data from magnetic stripe on the card);
- Computer (used to download card user data from the skimmer);
- Black card stock (used to create cloned cards);
- Magnetic stripe reader-writer (used to add data downloaded from computer to blank card);
- Card printer (used for adding artwork to blank plastic cards);
- Visa hologram sticker (optional – used for some credit cards); and
- Embosser (used for adding user name, account number, expiration date on cloned cards).

Major Handheld Skimmer Fraud Schemes

The following is a snapshot of a recent major handheld skimmer fraud scheme:

$2.2 million+ – November 2011, criminal network involved waiters and waitresses using handheld skimmers at restaurants in New York City, including Smith & Wollensky, The Capital Grille, Wolfgang's Steakhouse, and JoJo.

XIV. Helpful Online Resources

The Web features a number of helpful websites when researching skimmer scams. Among the ones that we proved resourceful to identify trends incidents and data were the following:

1. United States Secret Service (USSS) / Electronic Crimes Task Force (ECTF)
URL: www.secretservice.gov/ectf.shtml

Overview: Under the U.S. PATRIOT Act of 2001, the United States Secret Service (USSS) was mandated to create a network of Electronic Crimes Task Forces (ECTF). An ECTF brings together federal, state and local law enforcement to pool resources and work together on cases involving financial crimes. The USSS are considered the foremost authority when it comes to investigating skimmer fraud in the United States.

2. European ATM Security & Fraud Prevention
URL: www.european-atm-security.eu/

Overview: EAST (European ATM Security Team) is a non-profit organization committed to providing awareness of crime involvement payment systems in Europe, with a particular emphasis on ATMs, and ultimately providing for improvements in security. The membership of EAST represents 29 countries with a total of 625,776 ATMs.

3. ATMsecurity.com
URL: www.atmsecurity.com

Overview: The Website provides news on ATM fraud and ATM security. It is an excellent source of information – especially for those who want to get daily updates on ATM fraud and security issues.

4. Krebs on Security
URL: krebsonsecurity.com/all-about-skimmers/

Overview: Former editor for the Washington Post, Brian Krebs, now has his own security consulting firm. He has written extensively in his blog about skimmer technologies currently being developed and used by criminals.

5. Federal Bureau of Investigations (FBI)
URL: www.fbi.gov

Overview: Established in 1908, the FBI has a budget of $8.1 billion and 36,000 employees. Their mandate is threat intelligence and law enforcement. The FBI regularly partners with other law enforcement agencies on skimmer fraud investigations – especially because many of these investigations are intra-state crimes.

6. ATM Industry Association (ATMIA)
URL: www.atmia.com

Overview: Established in 1997, this non-profit trade organization has membership of more than 3,700 hundred members in 60 countries and those members represent more than 2.2 million ATMs. The group provides the latest news about the ATM industry to its members. ATMIA also issues reports based upon surveys of its own members.

7. ATM Marketplace
URL: www.atmmarketplace.com

Overview: ATM Marketplace is not only a source for the latest news but also provides invaluable information about industry changes and concerns, including the introduction of EMV compliant ATMs in the United States.

8. Europol
URL: www.europol.europa.eu

Overview: Europol is the European Union's law enforcement agency, which is involved in fighting crime, including terrorism, international drug trafficking, Euro counterfeiting, human trafficking and cybercrime. The recently established European Cybercrime Centre (EC3) has been established to fight online criminal activity. Skimmer fraud in the EU is largely perpetrated by organized crime gangs working across many countries in Europe and therefore Europol is very active in skimmer fraud investigations.

9. Aite Group
URL: www.aitegroup.com

Overview: The Aite Group is a research and advisory firm that focuses on the financial industry. Its research provides subscribers with information about market trends, which has included statistics relating to skimmer fraud.

10. STOPFRAUD.gov
URL: www.stopfraud.gov

Overview: In November 2009, the Financial Fraud Enforcement Taskforce was established by President Obama in response to financial fraud of immense proportions, from the mortgage crisis to Ponzi schemes. This organization represents 20 federal agencies, 94 US Attorney Offices and state and local partners.

XVI. About Us

About Dr. Darren Hayes

Darren Hayes is a graduate of University College Dublin, Ireland and Pace University, New York. Hayes spent more than a decade employed in the financial services industry in New York City and subsequently worked for a decade in information technology. He is an Assistant Professor at Pace University, New York. He is a leading expert in the field of digital forensics and cyber security. In 2013, he was listed as one of the Top 10 Computer Forensics Professors by Forensics Colleges. Hayes has appeared on Bloomberg Television, The Street and Fox 5 News and been quoted by CNN, The Guardian (UK), The Times (UK), Financial Times, Forbes, Investor's Business Daily, MarketWatch, CNBC, ABC News, Forensic Magazine, SC Magazine, PC Magazine, USA Today, Washington Post, New York Post, Daily News and Wired News to name but a few.

Hayes has developed a computer forensics program at Pace and has created a computer forensics research laboratory at the Seidenberg School of Computer Science and Information Systems. Hayes continually conducts research with students at Pace in support of law enforcement agencies domestically and internationally. As a practitioner, he has worked on numerous cases involving digital evidence related to both civil and criminal investigations. He is also a professional consultant in computer forensics and cyberlaw for the Department of Education. Hayes is also an accomplished author and is looking forward to publishing his third book in 2014 entitled "A Practical Guide to Computer Forensics Investigations".

About ACCA USA

ACCA USA is ACCA's headquarters stateside. ACCA USA was formally established in California in 1987, when 280 members and 193 students were living in the United States. Through our membership support, educational infrastructure, and forward-thinking research, we offer top-quality training, qualifications, networking opportunities and resources for career advancement to the global finance leaders of today and the CFOs of tomorrow.

Our finance and accounting professionals gain membership through our internationally recognized ACCA qualification which offers the most up-to-date, relevant, and consistent accounting

qualification available, delivering finance and accounting knowledge and skills as well as professional values.

Beyond the qualification, ACCA USA's 11 national chapters are important forums for networking, job searching, and continuing professional development. Learn more about our USA Chapter Network or find out about upcoming Chapter Events.

Moreover, ACCA USA takes numerous actions on behalf of its members, working to conduct surveys and research while developing a wide roster of programs to enhance the organization's contributions to the finance and accounting profession and to its membership.

We believe that the future of accountancy depends on shaping public policy, as well as demonstrating thought leadership in education, training, and ethics. ACCA USA and its members ensure that this happens by playing key roles in building the global accountancy profession and working with many other bodies at international, regional, and local levels.

About Pace University

Since 1906, Pace University has produced thinking professionals by providing high-quality education for the professions with a firm base in liberal learning amid the advantages of the New York Metropolitan Area. A private university, Pace has campuses in New York City and Westchester County, enrolling almost 13,000 students in bachelor's, master's, and doctoral programs in its College of Health Professions, Dyson College of Arts and Sciences, Lubin School of Business, School of Education, School of Law, and Seidenberg School of Computer Science and Information Systems.

The Seidenberg School of Computer Science and Information Systems was named after its generous benefactor, Ivan G. Seidenberg, Chairman & CEO Verizon Communications, Inc. The Seidenberg School was founded in 1983 and provides an exemplary education to students at undergraduate, graduate and doctoral levels in various disciplines to meet the ever-changing needs of employers. It is the first school in the New York Metropolitan Area to be designated a National Center of Academic Excellence in Information Assurance Education (IAE) by the National Security Agency (NSA) and the Department of Homeland Security.