ORION FORUM

An Analysis of ATM and Point-of-Sale Skimming

APRIL 25, 2025

ATM and POS skimming is a recurring societal problem, especially with the changing technological world. Recently, police discovered ATM skimming devices at convenience stores in York County and Lancaster County[1]. In Philadelphia, Supplemental Nutrition Assistance Program (SNAP) benefits were compromised due to skimming devices[2]. Although these are three macro-level events, ATM and point-of-sale skimming attacks have similar victims, circumstances, perpetrators, and locations. Card shoppers and ATM users face the same effects from the same weapon – a skimmer – in monetary environments by money-motivated perpetrators. This is an acute, meticulous, yet harmful problem that leads to the victims and the extended community expecting law enforcement to address it.

Automated teller machines (ATMs) and point-of-sale (POS) systems are known monetary entities that society interacts with daily. With technology progressing, ATM and POS system skimming is a security problem that has led to “a global outcry”[3]. Providing software for computing a person’s credit score, a large company recently discovered a significant increase in skimming attacks from 2021 to 2022. FICO announced a 452% increase in POCs [skimming points of compromise] from 2022[4] . This surge makes it important to stay vigilant and observant when utilizing ATMs and POS systems. The current report provides legal and technical definitions of ATM and POS skimming, explains how perpetrators commit it, and proposes measures to prevent it from further occurrences.

Definition

On a broader scale, ATM and POS skimming is a specific form of computer fraud and theft. The skimmer intends to “*extort…any money or other thing of value*…” and “*obtain information*

from a protected computer without authorization...or to impair the confidentiality of information obtained...without authorization or by exceeding authorized access."[5] (18 U.S.C. 1030). To put it another way, skimming is "*the activity of illegally duplicating information contained in a magnetic stripe found on a credit or ATM/debit card with a device known as a skimmer*"[6] (Dewi & Septiwidiantari, 2021, p.107). This crime fits into multiple aspects of the computer fraud and theft criteria that the United States Code has delegated. ATM and POS skimming is a form of cybercrime that evolves alongside technology. Although this crime fits the criteria for computer theft and fraud, it is similar in behavior to three other crime events – Trojan Horse attacks, identity theft, and embezzlement. Trojan Horse attacks are deceitful cyber-attacks that appear non-threatening but are malicious. ATMs and POS systems appear normal, but malicious skimmers capture and transmit financial data. With compromised information, perpetrators can steal one's identity (identity theft) and money (embezzlement) through cloned cards[7].

Modus Operandi

Skimming evolves in four phases: obtaining a device, installation, data capture, and fraudulent use of captured data. To begin with, skimming utilizes a camouflaged counterfeit card reader that records the data from a credit, debit, or ATM card and copies the data onto a blank card that the perpetrator(s) uses to obtain money from the victim's account[8]. When a credit, debit, or bank card is slid into an ATM or POS system that has a skimmer attached, the counterfeit reader scans the information stored in the card's magnetic stripe and stores it. From here, the captured data can be used to withdraw cash from the victim's account[9]. Through a simple device, ATM and POS users are targeted by offenders who desire a quick payday.

ATM and POS skimming, and computer fraud and theft deal with the digital realm and illegally obtaining private financial information. With skimming, there is an additional physical component – the skimmer. Skimmers are manmade scanning devices used to "*access, read, obtain, memorize, or store ...information encoded on a payment card without the permission of the authorized user...or with the intent to defraud the authorized user, another person, or a financial institution*"[10]. According to the Federal Bureau of Investigation (FBI), "*skimming*

occurs when devices illegally installed on or inside ATMs, point-of-sale (POS), or fuel pumps capture card data and record cardholders' PIN entries"[11].

For Kasanda and Phiri (2018), a skimmer is a hidden card reading device that reads data from the card's magnetic stripe or EMV (Europay, Mastercard, Visa) chip after insertion[12]. The skimmer acts as "the man in the middle" with the perpetrator(s) and victim(s) on opposite ends. The offender obtains the user's card information from the skimmer without direct contact with the victim. There typically is no intermediary in traditional computer fraud and theft. It is simply the perpetrator launching a digital attack against a target, but in ATM and POS skimming, the perpetrators are not really interested in who and what is targeted and affected – money is the prize.

Skimming devices are wireless, meaning captured information can be immediately transmitted or stored and transmitted later with no future interaction necessary to retrieve data[13]. The captured data can access additional funds or create "cloned cards," which are "*illegitimate cards using a legitimate user's stolen information*"[14].

A skimmer is also a manufactured technological device that is placed over the terminal's card reader and does not interfere with the normal checkout or withdrawal process. Skimmers record and pass the financial information to the normal terminal underneath[15]. The compromised data is then transferred to the offender, allowing them to access and drain the victim's bank accounts without the victim's knowledge. Using a skimmer and gathering information from it is part of the modus operandi or the crime's method of operation.

Skimming is not confined to physical, man-made devices; the crime can also be software-based. Silent skimmers are threats that infiltrate payment systems and exfiltrate payment information using Python scripts. These attacks utilize two vulnerabilities as common entry points – unrestricted file uploads and the enablement of remote code execution. Once access is gained and the attack can exert control over the system, the silent skimmer seeks to maintain a long-term presence within the organization through web shells, reverse shells, and PowerShell commands. When the skimmer has established its presence and obtained elevated privileges, it uses the embedded Python script to directly connect to the payment database, get the financial data, and further conceal its presence[16].

In this technological crime, skimmers are not the only devices used. Offenders may also use pinhole cameras and keylogging devices to gather account information. Pinhole cameras are tiny, watchful devices that often go undetected and allow the offender to capture the victim's personal identification number (PIN) without them knowing[17]. Keylogging devices can also be installed over the PIN pad and have software that captures the victim's strokes when typing in the four-digit code. Once compromised, the information may be sold to a third party or used to create cloned cards that withdraw funds directly from the victim's account[18]. This advanced and constantly progressing technological crime provides offenders with a big payday.

Skimming offenders may work alone or as part of a skimming ring, where higher-ups distribute orders[19]. When offenders work together, one person typically distracts the cashier or covers any security camera while the other lays the skimmer over the card terminal[20]. They may also compromise an employee by promising payment if they re-swipe a customer's card to ensure all financial information is obtained[21]. It is difficult to catch skimming offenders since they avoid close contact with their devices after installation. The offenders do not need to encounter the skimmer to obtain the data – the compromised information can be extracted from up to fifty yards away[22].

Skimming occurs wherever bank, credit, or debit cards are regularly swiped, such as cash registers, ATMs, and retail stores[23]. During the COVID-19 Pandemic, gas station pumps were the ideal location for skimming attacks, and they still are. They are automated and often left unattended, resulting in the loss of a place manager and granting the perfect opportunity for offenders to embed the device. Stand-alone ATMs in convenience stores may be more susceptible to skimming than bank-based ATMs[24]. Bank-based ATMs have pinhole cameras that function as potential capable guardians. These cameras may not exist in stand-alone ATMs, resulting in a loss of control and meaning no entity (i.e., CCTV surveillance, bystanders, and security personnel) is preventing crime.

In regard to timing, the skimming device is likely to be placed at night since there are fewer people around, allowing offenders to commit their crimes with a low chance of being caught. These attacks may happen more around the holidays since a lot of money and cards will

circulate in the economy. Once the device is placed, anyone is at risk at all times of day and year, and these attacks may never stop until the device is discovered. Also, offenders are aware of recent technological changes and know the security behind electronic money transfers is outdated, precipitating them to launch a skimming attack[25].

Skimming is a predatory behavior in retail and financial environments, such as banks, grocery stores, and clothing stores. ATM and POS users are targeted in these environments but are unaware they are victims since skimmers often go undetected. ATM and POS skimming offenders meticulously plan their attacks to avoid police detection. For example, skimmers are efficiently handmade to obtain information without being identified. They are placed efficiently to appear invisible to the naked eye. Those affected can lose their finances and fall victim to fraud since private financial information is compromised.

In brief, shopping malls, grocery stores, event venues, and gas stations can be settings of skimming. On days such as Black Friday, Thanksgiving Eve, or Christmas Eve, these places may lack control (i.e., security guards, employees, cameras), granting the perfect opportunities for skimming offenders. At these locations, various groups in different amounts are brought together, giving offenders the perfect and oblivious victim pool. Although they were not designed for crime, these locations generate and attract it.

Prevention

To prevent skimming from happening requires involving all stakeholders in preventive strategies, including card users, ATM and POS machine manufacturers, and security professionals. On an individual level, cardholders should examine the card reader before inserting it. If the card reader looks raised or bulkier, there might be a skimmer. If the greenish coloring on ATMs looks dull, there runs the risk of a skimmer. Users should also fiddle with the card reader by pulling or wiggling it to look for a loose-fitting attachment or a covering and scope the surrounding scene to check for any cameras with a clear sight of the PIN pad[26].

There are few technical interventions in place to prevent skimming, but one can avoid becoming a victim by being aware and vigilant of everything. Card users should carefully inspect an ATM or POS system before inserting their card. If they see any tampering, there is

the possibility of a skimmer. It is advised for the user not to insert or swipe their card if the reader seems loose, crooked, or damaged, or if the color is off. Users should also avoid using their cards at non-bank ATMs (i.e., bars, restaurants, convenience stores), and at ATMs and gas stations in desolate areas since they lack essential preventive controls. Since skimmers are not the only devices used in this crime's commission, users must check the PIN pad and surrounding areas. If the keys on the PIN pad feel hard to press or are thicker than usual, there runs the risk of a keylogging device. If everything about the ATM and POS system feels familiar, it is still critical for users to check the perimeter.

Users should take notice of any shady characters who are only in the same location as themselves for their PIN and inspect the walls of the ATM for any pinhole cameras. Users should always block their PIN and examine the machine before use[27]. Although all cards, chip-embedded or magnetic stripes, are prone to skimming attacks, it is in the user's best interest to use an EMV chip-embedded card. If there is a skimmer on an ATM or a point-of-sale system and the user taps their card instead of inserting it, their risk of becoming a skimming victim decreases. EMV chips generate unique transaction codes for every transaction, making it harder to clone these cards[28]. It is possible to avoid becoming a skimming victim, but it does take a lot of critical analyses before completing a transaction or withdrawal.

As mentioned before, there are few technical interventions in place to prevent this crime, but there are intelligent and advanced proposals. Al Rawahi and Nair (2015) proposed a semi-automated system to detect skimmers or other abnormal ATM attachments through image processing[29]. The system uses machine learning algorithms to detect suspicious devices. It compares images of ATMs to a database of normal configurations. By detecting unusual patterns or shapes, the system is able to identify foreign objects such as skimmers, cameras, or other tampering devices. Although the system is not universally adopted yet, Target has recently begun to use it to detect skimming devices on its payment terminals[30].

Another intervention in skimming problem was presented by Kumar and colleagues (2021)[31]. They proposed cardless ATMs that rely on biometrics to obtain a user's financial information. The user will start with fingerprint identification and facial recognition, which is converted into digitized code and stored in a protected database. When interacting with the ATM, a user's

face and fingerprint will be cross-checked with the machine's registered biometrics. If approved, the user will be prompted to enter a one-time password sent to their phone, confirming their identity and granting them access to their monetary funds[32].

A new plan of action, which combines the two previous proposals, could be proposed to combat skimming. Before and during current interventions, offenders placed skimming devices while being surveilled, meaning that any watchful eyes (i.e., bystanders, cameras, and security guards) would not stop them. To intervene with the problem, it would be efficient for tech companies, such as Diebold Nixdorf, Inc., NCR Corporation, and Triton Systems of Delaware LLC, to create cardless and biometrically secure ATMs and POS systems since they have biometrics, software, hardware, and security expertise. These are some of the top companies for ATMs and POS systems that can implement this intervention.

From a forensics standpoint, finding skimmer flaws that may go undetected from far away but are noticeable upon a thorough inspection will also be useful. To further explore this problem, it would be useful to install more pinhole cameras that are completely undetectable, have high radiance, and send surveillance in real time to catch offenders before further harm has been caused.

The crime of skimming requires proactive intervention, meaning that preventive measures must be taken beforehand. For the most part, ATMs and POS systems have closed-circuit television (CCTV) cameras watching them. Although having cameras is a promising idea for crime deterrence, businesses and banks only refer to these cameras after a problem arises, rather than having them be constantly surveilled[33]. CCTV cameras need a constant watchful eye to be effective in deterring skimming. Another current implementation is having scan-only access to banks. Only cardholders are supposed to gain access to the building, but they are not always aware of who is following close behind them. These everyday citizens may hold the door open for a skimming offender who has the power to affect others for days, months, or years. For these reasons, ATM and POS machine operators should be trained on regularly checking and detecting if there are any skimmers placed in any device.

Summary of Preventive Strategies

Users:

Inspect an ATM or POS machine

Avoid non-bank ATMs

Check for any pinhole cameras on the walls around ATMs

Use an EMV chip-embedded card

Manufacturers:

Embed a semi-automated system to detect skimmers

Adopt cardless ATMs relying on biometrics

Place ATMs in well-lit, well-maintained, and properly surveilled areas.

Operators:

Get training on checking and detecting a skimmer

End Notes

[1] Kaylee Lindenmuth, “Police Warn about Skimming Devices Placed on ATMs,” *ABC27*, August 3, 2024, www.abc27.com/local-news/police-warn-about-skimming-devices-placed-on-atms/; Brady Doran, “Skimming Device Found at Lancaster County Gas Station,” *ABC27*, September 12, 2024, www.abc27.com/local-news/skimming-device-found-at-lancaster-county-gas-station/.

[2] Brandon Thomas, “DHS Reminds Pennsylvanians to Be Alert for Skimming Devices,” *WTAJ*, June 9, 2024, https://www.wtaj.com/news/regional-news/dhs-reminds-pennsylvanians-to-be-alert-for-skimming-devices-that-steal-your-information/.

[3] Paramjit Kaur et al., “ATM Card Cloning and Ethical Considerations,” *Science and Engineering Ethics* (2019), https://doi.org/10.1007/s11948-018-0049-x.

[4] Debbie Cobb, “US Card Skimming Grew Nearly 5x in 2022, New FICO Data Shows,” *FICO Decisions Blog*, February 16, 2023, www.fico.com/blogs/us-card-skimming-grew-nearly-5x-

2022-new-fico-data-shows#:~:text=For%202022%2C%20we%20saw%20a,had%20not%20been%20compromised%20befor
).

[5] "18 USC § 1030: Fraud and Related Activity in Connection with Computers," *United States Code,* https://uscode.house.gov/view.xhtml?req=%28title%3A18+section%3A1030+edition%3Aprelim%29 .

[6] Putu Eka Trisna Dewi and Ni Made Septiwidiantari, "Efforts to Overcome Criminal Acts of Skimming Committed Through ATMs in the Perspective of Law Number 19 of 2016 Concerning EIT," *NOTARIIL Jurnal Kenotariatan,* 6 (2): 107.

[7] S. Shaw, "Skimming: Attacking Your Financial Security," December 13, 2019, www.cs.tufts.edu/comp/116/archive/fall2019/sshaw.pdf.

[8] Mohamed Musallam Khasib Al Rawahi and Smitha Sunil Kumaran Nair, "Detecting Skimming Devices in ATM Through Image Processing," *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, November 2015, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7507139.

[9] Northwest Community Credit Union (NCCU), "How to Spot an ATM Skimmer," *Northwest Community Credit Union*, https://www.nwcu.com/learn/how-spot-atm-skimmer.

[10] "RCW 9A.56.290: Credit, Payment Cards – Unlawful Factoring of Transactions," *Revised Code of Washington*, https://app.leg.wa.gov/rcw/default.aspx?cite=9A.56.290.

[11] Federal Bureau of Investigation (FBI), *Skimming*, n.d., https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/skimming.

[12] Ella Nsonta Kasanda and Jackson Phiri, "ATM Security: A Case Study of Emerging Threats," *International Journal of Advanced Studies in Computers, Science and Engineering*, 7.10 (2018): 1, https://www.proquest.com/docview/2161593902?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals.

[13] FBI, *Skimming.*

[14] Shaw, “Skimming: Attacking Your Financial Security,” 2.

[15] Jessica Fu, “The Skim Scam,” *Bloomberg Businessweek*, no. 4789 (2023): 52-57.

[16] Guardians of Cyber, “Silent Skimmer Exploits Telerik Flaws to Drain Payment Systems,” *Guardians of Cyber*, November 10, 2024, https://guardiansofcyber.com/threats-vulnerabilities/silent-skimmer-flaws/.

[17] Lisa Gerstner, “Watch out for Skimming Scams,” *Kiplinger’s Personal Finance,* 67.9 (2013): 61.

[18] Hayder Hussien Aziz, Saif Mohammed, and Ali Taha Yaseen, “Factors of Implementing Biometric Security on Measure of ATM,” *International Journal of Engineering and Technical Research,* 3.5 (2015): 491-498.

[19] Federal Bureau of Investigation (FBI), “Romanian Police Serve Dozens of Warrants Following Parallel Investigation with the FBI’s Los Angeles Field Office,” *FBI*, February 14, 2025, https://www.fbi.gov/contact-us/field-offices/losangeles/news/romanian-police-serve-dozens-of-warrants-following-parallel-investigation-with-the-fbis-los-angeles-field-office.

[20] FBI, *Skimming.*

[21] Gerstner, “Watch out for Skimming Scams,” 61.

[22] Scott H. Belshaw et al., “Skimmed at the Pump: How COVID-19 Lockdowns Increased Gas Pump Skimming,” *Crime & Delinquency,* 68.8 (2022): 1207-1222, https://doi.org/10.1177/00111287221081028.

[23] Fu, “The Skim Scam.”

[24] Mukesh Sharma and Shailendra Jha, “Digital Data Stealing from ATM Using Data Skimmers: Challenge to the Forensic Examiner,” *Journal of Forensic Sciences & Criminal Investigation,* 1.4 (2017): 552-567, https://doi.org/10.1177/00111287221081028.

[25] Fu, “The Skim Scam.”

[26] NCCU, “How to spot an ATM skimmer.”

[27] First United Credit Union (FUCU), “Ten Tips to Prevent Card Skimming Fraud,” *1st United Credit Union,* n.d., www.1stunitedcu.org/more-for-you/financial-wellness/ten-tips-to-prevent-card-skimming-fraud.

[28] DataVisor, “What You Need to Know about Card Skimming Scams,” *DataVisor*, n.d., www.datavisor.com/wiki/card-skimming/#:~:text=Can%20Chip%20Cards%20be%20Skimmed,readers%20and%20skim%20that%20w
.

[29] Mohamed Musallam Khasib Al Rawahi and Smitha Sunil Kumaran Nair, “Detecting skimming devices in ATM through image processing.”

[30] Terry Woodman, “Cybersecurity: EasySweep,” *Target*, July 18, 2023, https://tech.target.com/blog/cybersecurity-easysweep?utm_source=chatgpt.com.

[31] M. Navin Kumar et al., “Biometrically secured atm vigilance system,” *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 1, 919–922, https://ieeexplore.ieee.org/document/9441975.

[32] M. Navin Kumar et al., “Biometrically secured atm vigilance system.”

[33] Mohamed Musallam Khasib Al Rawahi and Smitha Sunil Kumaran Nair, “Detecting skimming devices in ATM through image processing.”