European Perspectives – International Scientific Journal on European Perspectives
Volume 15, Number 1 (27), April 2024, pp. 19-40

ATMs and Their Security

Franc Pozderec, Tomaž Čas, Ivanka Oberman[1]

DOI: *https://doi.org/10.60073/euper.2024.4.03*

ABSTRACT

Automated teller machines (ATMs) are devices that enable users to provide banking services and are an indispensable part of modern banking services. They have the advantage of being constantly operational and, unlike a bank, are available to users at all times. As the number and use of ATMs has increased, so have the various types of misuse of these machines, where perpetrators attempt to obtain property or user data in various ways. Attacks can target ATMs, users or banks, and can be divided into traditional abuse based on the use of physical force to access a security container, and abuse that exploits the data of the cards used or affects the operation of the ATM itself. Knowledge of the ways in which ATMs are misused has a significant impact on minimising damage; as well the intensive development of protective mechanisms on ATMs is an important aspect of ensuring the security of using ATMs.

The article outlines the known types of abuse, their frequency, some of the options for action and the mechanisms banks use to protect their own and their customers' assets.

KEYWORDS: ATMs, historical development, abuse, cash, data, security

POVZETEK

Bankomati so naprave, ki uporabnikom omogočajo opravljanje bančnih storitev in so nepogrešljiv del sodobnih bančnih storitev. Njihova prednost je ta, da omogočajo nenehno delovanje in so, v nasprotju z banko, uporabnikom dosegljive ves čas. Ob naraščanju števila in rabe bankomatov naraščajo tudi različne vrste zlorab teh naprav, kjer si storilci na različne načine poskušajo pridobiti imetje ali podatke uporabnikov. Napadi so lahko usmerjeni na bankomate, uporabnike ali banke, torej delimo jih na klasične zlorabe, ki temeljijo na uporabi fizične sile za dostop do varnostnega vsebnika, ter na zlorabe, ki izkoriščajo podatke uporabljenih kartic ali vplivajo na delovanje samega bankomata. Poznavanje načinov zlorab bankomatov pomembno vpliva na minimaliziranje škode, prav tako pa intenziven razvoj zaščitnih mehanizmov na bankomatih predstavlja pomemben aspekt zagotavljanja varnosti uporabe bankomatov.V članku so predstavljene poznane vrste zlorab, njihova pogostost, nekatere možnosti ukrepanja in mehanizmi, ki se jih poslužujejo banke, da varujejo svoje in premoženje uporabnikov.

KLJUČNE BESEDE: bankomati, zgodovinski razvoj, zlorabe, gotovina, podatki, varovanje

1 ABOUT THE AUTHORS:
Franc Pozderec, PhD in Administrative Sciences, Assist. Prof. of Administrative Law, European Law Faculty, New University Slovenia and at the Faculty of Government and European Studies, at the Police college within the Police Academy, Email: *franc.pozderec@gmail.com*
Tomaž Čas, PhD in Defense Studies, Assoc. Prof. of Security System, Faculty of Security Sciences, European Faculty of Law, and Faculty of Government and European Studies, New University, Slovenia. Email: *tina.cas@siol.net*
Ivanka Oberman, M.A. of Law, European Faculty of Law, New University, Slovenia, Email: *ivana.oberman@gmail.com*

Introduction

An automated teller machine (hereinafter ATM)[2] is an electronic telecommunications device that allows you to complete financial transactions, such as cash withdrawals, deposits, funds transfers, balance inquiries or account information inquiries, at any time and without the need of a bank representative. Many ATMs are conveniently accessible any time of day or night and can be used for everything from withdrawing or depositing money, checking your account balance to transferring money between accounts. Using an ATM simply involves inserting your bank-issued ATM card, entering your personal identification number (PIN)[3] and following the prompts on the screen to complete your desired transaction (Bennet, 2023).

The design of each ATM may be different, but they all contain the same basic parts (Kagan, 2023):

- Card reader: This part reads the chip on the front of your card or the magnetic stripe on the back.
- Keypad: The keypad is used to input information, including your personal identification number (PIN), the type of transaction required, and the amount of the transaction.
- Cash dispenser: Bills are dispensed through a slot in the machine, which is connected to a safe at the bottom of the machine.
- Printer: If required, you can request receipts that are printed out of the ATM. The receipt records the type of transaction, the amount, and the current account balance.
- Screen: The ATM issues prompts that guide you through the process of executing the transaction. Information about accounts and their balances is also transmitted on the screen.
- Full-service machines often have slots for depositing paper checks or cash.

An ATM consists of a card reader, a keypad, a screen, a money feeder, a printer, a money safe and a computer (Bowen, 2000, p.4). First, a card is inserted into the slot of the card reader, which has the user's information stored on a magnetic stripe or chip. The ATM then asks for a PIN, which is entered via the keypad. The keys next to the screen are used to select the desired activity, after which the option to print out

2 ATM is an abbreviation for automated teller machine: a machine, usually outside a bank, which customers can use to get money out or manage their account by using a plastic card together with a PIN (a secret number).

3 PIN (a personal identification number) is a unique combination of numbers that only the account owner knows and it is a form of authentication that adds an extra layer of security to our accounts.

a service receipt is offered. In the case of cash withdrawals, the money stored in the cassettes in the safety deposit box is withdrawn from the cash dispensing slot. Before this, the card must be removed from the ATM. At the end, a receipt is printed (Klinar, 2006, pp.22-27).

The services offered by ATMs to users are increasing with continuous development, including (Bankart, n.d.):

- an automatic cash deposit;
- an electronic payment of universal payment orders (UPOs);
- a quick cash withdrawal;
- a withdraw the amount of your choice;
- a statement of the turnover on your personal account;
- an access to your personal account balance;
- a PIN change;
- a purchase of Global system for mobile communications cards (GSM);
- an access your credit card balances;
- an order for a cash deposit;
- an order for the settlement of payment orders.

Banks can impose ATM withdrawal limits out of practicality and for security reasons. First, ATMs can hold only so much cash, and banks have only so much cash they can distribute to customers at any given time. Setting an ATM withdrawal max for each customer helps the bank control the movement of available cash. The other reason has to do with security and protecting customer accounts. In case someone stole your debit card and PIN, without an ATM withdrawal limit, they would be able to drain your checking or savings account and pocket all your cash (Lake, 2022).

It is known that banks usually place ATMs inside and outside of their branches. Other ATMs are located in high-traffic areas such as shopping centers, grocery stores, convenience stores, airports, bus and railway stations, gas stations, casinos, restaurants, and other locations. Also, ATMs make it easier for people to access their checking or savings accounts from almost anywhere in the world where they travel (Kagan, 2023).

For small companies that can feasibly have them installed and maintained, ATMs placed in well-trafficked locations have been shown to offer several business benefits. Those include opportunities for the

business to obtain revenue through transaction fees; higher rates of on-premises spending by consumers using the machines; reductions in costs and service time related to processing credit and debit card transactions; and additional ways to interact with the consumer through the ATM itself (Hirsh, n.d.).

Development and Operation of ATMS

European, American and Japanese bankers are responsible for the development of ATMs. They came to the realization that it would be very convenient for individuals to be able to access cash outside bank opening hours. Thus, in the United States of America (hereinafter USA), ticket offices, vending machines and unmanned petrol stations proliferated in the 1950s and 1960s. These types of machines dispensed a paid product to an individual who inserted the required amount of money. Based on this, the bankers assumed that withdrawing cash from accounts could be done in the reverse of the operation of the devices listed above (Huš, 2015).

The first device that could be described as a precursor of today's ATMs was installed in 1960 by a bank in New York (Harper, 2004), called the Bankograph[4], invented by Luther George Simjian (Batiz-Lazo and Reid, 2008, p.111). Due to insufficient interest, the device was withdrawn after six months. On 27 June 1967, the first European cash-only ATM was installed in a suburb of London by Barclays, designed by John Shepherd-Barron. It used special cheques designed for one-off use. The user also had to identify himself with a four-digit personal identification number (PIN). In 1969, the first cash dispenser to accept plastic cards with a magnetic stripe was installed. In 1971, the Docutel company installed the first true multi-function ATM in the USA (Miller, 2011).

The first ATM in Slovenia was installed on 8 February 1990 at Ljubljanska banka (hereinafter LB). LB, together with some other Slovenian banks, continued to develop its ATM network, and in 1993 a group of banks, led by bank SKB, entered the market. In 1997, the two ATM networks merged, and the banks jointly established Bankart, which has been operating ATMs in Slovenia since then (Klinar, 2006, pp.28-30). Bankart operates 95% of all ATMs in Slovenia.

4 The Bankograph accepted cash and check deposits. It used a camera inside the machine to take snapshots of the deposits, copies of which were given to the customers as receipts. Bankographs were installed in several branches of the City Bank of New York, but the machines were removed after six months due to limited use. It seemed few customers were willing to trust their money to a robot.

Table 1: Number of ATMs in Slovenia

Year	Number of ATMs
2011	1845
2012	1789
2013	1775
2014	1692
2015	1690
2016	1676
2017	1646
2018	1580
2019	1545
2020	1406
2021	1443

Source: Bank of Slovenia Bulletin (n.d.).

In 2017, Nova ljubljanska banka (hereinafter NLB) introduced and activated two contactless ATMs. The ATM has a specially marked area where the bank card is inserted. A PIN number is then entered. This makes it even faster and easier for users to withdraw cash and check their account balance. By the end of 2018, 250 such ATMs should be installed and activated. Intesa Sanpaolo Bank already allows users to withdraw cash via mobile phone (Ropret, 2017).

Table 2: Number of ATM withdrawals in Slovenia

Year	Withdrawals with cards of domestic issuers - at ATMs owned by the card issuers	Withdrawals with cards of domestic issuers - at ATMs not owned by the card issuers	Withdrawals with cards of foreign issuers
2015	33.852.126	20.291.804	1.066.466
2016	32.526.953	20.018.848	3.368.917
2017	34.031.395	19.192.034	3.299.467
2018	33.448.309	19.400.978	3.495.642
2019	32.369.596	19.474.459	3.581.115
2020	26.184.127	14.962.321	2.533.677
2021	26.532.976	13.393.656	2.485.351

Source: Bank of Slovenia Bulletin (n.d.).

As can be seen from Table No.2, the total number of withdrawals, both with cards of domestic banks and with cards of foreign banks, decreased significantly in 2020 and 2021. Whereas in the previous five years the number of withdrawals was approximately the same. In all likelihood,

the decline is due to the Covid-19 epidemic, which has forced people to use more cashless transactions. Other possible reasons include the introduction of fees for withdrawing cash from another bank's ATM and the increasing use of online and mobile banking.

In 1999, the first talking ATM for blind people and people with visual impairments made its public debut at San Francisco City Hall. Today, there are more than 100,000 of these machines in operation in the United States, with more coming all the time, and they can be found in nations all over the world. ATMs for the visually impaired include Braille, both on the keys and Braille instructions. The keys of an ATM are designed in a certain way to assist the blind. Keys are raised and the numbers are set up in a way that makes them easy to find. These ATMs deliver through voice recordings all the information that seeing customers read. Visually impaired people listen to ATM voices through headphones. Senior citizens who are not legally blind but who have issues with their eyesight can derive benefit from talking ATMs. These machines also provide assistance to people who are illiterate or who have reading disabilities (Wieder, n.d.).

In 2023, Slovenian bank Nova ljubljanska banka has adapted some ATMs so that they can be used by blind people and people with visual impairments. Voice guidance at the ATM is in Slovenian language and it starts when the program detects that the headset is activated and connected to headphone jack on the ATM. Some features of the ATMs have also been adjusted, such as the keys on the dial, side keys with Braille, larger elements and also the contrast of the screen. For the blind and visually impaired people this is a new step towards a more independent life (Ropret, 2023).

Atm Attacks and Fraud

Despite their long presence on the market, ATMs are still prone to various types of abuse. According to data from the US, the number of payment card frauds (they do not collect separate data for card usage at ATMs and Point of Sale terminals (POS))[5] increased sixfold in 2015 and by an additional 30% in 2016. This does not include ATMs that were remotely hacked via malware. Global trends are also expected to show

5 POS-terminals (from the English Point of Sale) are autonomous devices that include hardware and software to process customer payments, record sales data, manage inventory and more. They can integrate numerous features to help the business run smoothly, including sales reporting and customer loyalty programs (Dublino, 2024).

an increase in abuse. According to some data from the US, this type of abuse is ten times more effective than robberies of the branches themselves, with the latter resulting in an average of USD 3 000-5 000 before the perpetrators are caught, and ATM abuse between USD 30 000-5 000. This also comes at the expense of the fact that chip technology has not been introduced in the US for a long time, as it is significantly easier to obtain a magnetic stripe record than a chip (Crossman and Ghosh, 2017).

In this article, we will look at the different types of abuse at ATMs. The range of possible abuse ranges from purely physical attacks on ATMs, to theft of user data at the ATM itself, or remote attacks on ATMs that then start dispensing money (Crossman and Ghosh, 2017). ATMs provide perpetrators with direct access to cash and, in some cases, to personal data that can be used for identity theft. While ATMs can contain a significant amount of cash, bank cards allow perpetrators to access users' bank accounts, and the sums in the accounts can easily exceed the value of the cash contained in a single ATM. As ATM attacks have been carried out, perpetrators have thus increasingly focused on ways to obtain bank card data (ENISA, 2009, p.12).

The shift from physical to digital ATM fraud suggests that perpetrators see this as an easier and safer way to obtain cash and the data stored on the cards. It can therefore be assumed that these modes of attack will continue to escalate (Geller, 2016).

Skimming

Skimming is still the most common form of ATM fraud. It involves the use of devices (readers) that capture data from the magnetic recording of the card. The readers are placed on the card slot or in the throat or inside the card reader. In addition, a PIN retrieval device is also installed. Users insert their card into such a reader and usually complete the transaction and receive the card back without being aware that the device has in the meantime captured the magnetic stripe data. After a certain period of time, the device is removed and the data is transferred to the computer. The data collected is used to create counterfeit cards for later fraudulent withdrawals. Users only become aware of the fraud after these withdrawals are made (ENISA, 2009, pp.14-15).

The technology to record on cards has improved dramatically and card

readers have become cheaper. As they are also used for purely business purposes, they are not illegal unless used for criminal purposes (Crossman and Ghosh, 2017).

Getting a PIN

The acquisition of a PIN number is a form of misuse that is overwhelmingly linked to one of the other forms of misuse of card acquisition or card data (Lamberger, 2011, p.61):

- an over-the-shoulder look is a method of obtaining a PIN where the perpetrators are in close proximity to the victim and observe intake;
- fake cameras installed on and near ATMs, for example on painted or taped above the keyboard;
- a fake keyboard that is placed on top of a real keyboard and stores the numbers in a memory unit.

The Money Trap

The money trap[6] is a manipulation of the cash-out system so that users do not receive the money that has been paid out and the account has been debited for that amount. These can be devices placed on the outside or inside of the cash dispensing mechanism. If it is installed externally, the perpetrators take the money as soon as the user leaves the ATM, whereas if it is installed internally, it is possible for the device to hold the money of several users (E.A.S.T., n.d.).

Reversal of a Transaction (Transaction Reversal)

This is a situation where the perpetrators get the ATM to detect that the cash has not been withdrawn (even though the perpetrator collects it) and report an error, and the transaction is reversed so that the perpetrator's account is not debited for the amount withdrawn. This can be achieved by physical manipulation of the payout system or through software that influences the error message that the cash has not been paid. In order to carry out the abuse, the perpetrator must have a valid card and sufficient funds in the account to attempt the withdrawal (E.A.S.T, 2018).

6 There are several warning signs to identify a cash trapping scam, including a damaged or tampered ATM cash slot, unexplained failure to dispense cash, or irregular timing in the cash release process (Negg Blogg, 2024).

Trojan Horse - Fake ATM

A Trojan horse[7] or fake ATM is an ATM that looks like a real ATM and some of them even dispense cash. This is how the perpetrators try to get hold of the PIN and the magnetic stripe on the cards. The ATM returns the card to the user after the PIN has been entered and the magnetic recording has been made, but tells the user that there is no money in the ATM. They only need a source of electricity to operate as they are not connected to the mains and can therefore be installed in many locations (ENISA, 2009, p.15).

Shimming

Shimming is analogous to skimming, except that it is the interception or manipulation of information transmitted between a Europay, Mastercard, Visa chip-enabled card and the chip reader in the card reader. The perpetrators use a small, paper-thin device which is placed in the card reader and inserted in such a way that it is between the card chip and the interface of the card reader. This can make its presence very difficult to detect. The device is then used by the perpetrators to harvest the recorded data, but they can only use it to create cards with a cloned magnetic stripe, not the chip itself, as this is not possible due to its composition and security mechanisms. Users can also avoid this type of abuse by using a contactless card. Additionally, a device is installed to obtain the PIN, such as a camera or an overlay on a PIN keypad (MacDonald, 2017).

Black Box

This type of abuse is a type of ATM attack, where the perpetrators use various means to gain access to the inside of the ATM. Some kind of a device, usually a laptop computer, is connected to the cash-feeding unit. This device then sends a signal directly to the cash dispenser to withdraw the money, bypassing the need to confirm the transaction. The perpetrators gain access to the ATM by drilling holes or melting it so that they can physically connect this additional device to the ATM. The losses can be significant, as this is how perpetrators withdraw all the cash that is in the ATM (Europol, 2017).

7 *Trojan horse* – it is a type of malware that is often disguised as legitimate software. The term was coined from the Greek myth of the wooden horse that was used to sneak into the city of Troy.The user is tricked into believing that the Trojan is a harmless program, thereby unwittingly inviting the malware into the system (McAfee, 2024).

Card Theft

Card theft involves various forms of abuse, the main purpose of which is to obtain a card for later use. One of the methods used to obtain the PIN is also used. Card trapping is a method where the perpetrators physically manipulate the ATM to prevent the card from being returned to the user. A device is applied over or inside the card slot to allow the card to pass through before the user has completed the transaction. The device shall retain the card at the ejection point after the transaction. After the user has left, the perpetrators shall remove the entire device together with the card, which shall then be used. The most well-known method is the so-called Lebanese loop, where a strip or wire is inserted into the card reader (E.A.S.T., n.d.).

Data Attacks

The target is the software and communication systems of ATMs/banks. They can cause significant damage and quickly compromise large amounts of data. The transition from proprietary operating systems of ATM manufacturers to the Microsoft Windows platform has also facilitated abuse. Different types of malware are used, which can be used locally (on the ATM itself) or remotely. They are often very difficult to detect as they are constantly evolving and changing. Remote attacks against banks' computer centres and servers that act as intermediaries between the bank and the ATM are mostly carried out by organised crime groups (Diebold, 2012). The use of malware targeting ATMs is gradually increasing, with the first cases reported in 2009 (Crossman and Ghosh, 2017).

Three of the methods of data attacks are jackpotting, man in the middle and software skimming. The perpetrators install malware in the ATM software either on-site or remotely over a network. On-site control of the malware is achieved by using electrical wiring to enter a PIN, by accessing unsecured communication interfaces such as a univert serial bus, or by running an unauthorised operating system. Jackpotting allows the perpetrators to control the dispensing of cash from an ATM. Man in the middle targets the communication between the ATM PC and the host system in order to falsify responses and dispense cash without debiting the perpetrator's account. Software skimming is designed to extract card data and PIN numbers to counterfeit cards, similar to conventional skimming, ex-

cept that the data is attempted to be extracted from the ATM itself (E.A.S.T., n.d.).

Another way of attack is through hacking into banks' systems. This is usually done by sending emails to bank employees that look like legitimate business communications, with an attachment that hides malware. When the employee opens the attachment, the software installs and allows the perpetrators to control the infected devices and access the banks' internal network. The perpetrators then infect ATM computers. They can then instruct them to withdraw cash at a specific time, when one of the gang members will be at the ATM to collect the money. This is therefore about harming financial institutions, not individual users (Geller, 2016). Similarly, members of the Russian-Ukrainian criminal gang that is believed to have carried out such attacks over the last five years with the Anunak, Carbanak and Cobalt malware have harmed 100 financial institutions for around €1.2 billion. They obtained the money not only through ATM withdrawals, but also through fake transfers to accounts they owned (Bing, 2018).

Physical Attacks

Physical attacks on ATMs are carried out to gain access to the cash in the ATM. The most common methods are (E.A.S.T., 2015, p.5):

- ATM break-ins, defined as a physical attack on an ATM at the point of installation - attacks can be carried out with brute force, cutting and sawing devices and explosive devices that can be used to blow up a safe;
- attacks on ATM cashiers while they are moving money in or out of the machine or during the cashing process itself;
- ATM theft, where the installed ATM is removed - the most common method of theft is by a motor vehicle collision.

ATM Safety and Security Recommendations

Attacks and abuse at ATMs cause losses for both users and ATM providers. For providers, preventing ATM abuse is a challenge to develop different ways and measures to secure ATMs to enable users to use them safely. Payment card security measures overlap with those of card issuers, whose desire is to successfully combine card performance (speed of use, reliability) with card security (Lamberger et al., 2012, p.124).

Perpetrators operate where they have fewer obstacles to achieving their goals. Every cardholder must be aware that they are jointly responsible for the assets in their bank account and that their security also depends on being aware of what they can do to use the ATM as safely as possible. As a result, ENISA (European Network and Information Security Agency) has made recommendations for the safe use of ATMs - the so-called "Golden Rules to reduce ATM-related crime" (ENISA, 2009, pp.24-25):

- your payment card must be handled with care, carried and stored securely;
- for security reasons, the cardholder should never give the card to someone else or entrust the PIN to them;
- the bank letter containing the PIN must be destroyed and the number should be memorised;
- the PIN and the card must not be stored together;
- the PIN must be changed at the ATM to one that each user can remember, so that there is no need to keep a record of it;
- make a note of the phone number of the card issuer, which can be used to report cancellations, loss or theft immediately;
- expired or cancelled cards must be destroyed;
- when using an ATM, you should pay attention to the specific features of the ATM (damage to the ATM slot, traces of sticky substances due to additionally installed devices, etc.) and the surrounding area (people who offer help in using an ATM, etc.).

The Association of Banks of Slovenia defines the following basic rules for the safe use of ATMs. The most important rules are highlighted below (Association of Banks of Slovenia, 2021):

- no-one should see the holder's PIN number when using the machine (if someone is standing nearby, the ATM user should ask them to move away; when entering the PIN, the keypad should be covered with both hands to prevent any recording);
- it is best to use your payment card at machines that are located in a well-lit and well-trafficked area;
- any irregularities or changes at the ATM must be stopped and the bank or the police should be informed as soon as possible;
- if the ATM does not return the card to the cardholder (due to an obstruction in the card slot) and there is a message on or next to the card stating that the PIN number must be re-entered, the user

should immediately inform the nearest bank branch or the police;
- if the ATM does not dispense cash despite the authorisation of the service, the account balance should be checked first; if the account holder finds that the account balance has changed or the amount requested has been authorised but not dispensed, the bank or the police should be informed immediately.

Physical Security

At the same time, the increasing use of ATMs in less secure locations has led to an increase in theft and vandalism (Weight, 2009, pp.4-17). Measures that banks are taking to protect themselves against these attacks include (Accenture, 2016, pp.23-25):

- appropriate fixing methods (in the floor, wall or ceiling) to make removal difficult;
- bollards to prevent ramming attacks;
- measures against attack by explosives or gas;
- installing an alarm device in the ATM itself;
- constant camera surveillance and sufficient lighting of the ATM;
- hiring security companies to respond quickly to an alarm or the presence of a security guard;
- a mirror to monitor the surroundings behind the user;
- a safe that meets security requirements;
- in the case of a high-risk location, the introduction of a cash limit in the safe;
- time-based locking of the room and installation of an alarm device (only for ATMs installed in a closed area);
- for particularly risky locations, the ATM can be additionally secured with chains,
- advertising security measures on the external visible signs of ATMs;
- installation of colour packs in tills;
- installing ATM locating devices - different types of devices are available, based on GPS (satellite), GSM (mobile network) and Radio Frequency (RF) technology;
- sensors to prevent skimming and card trapping;
- sensors to detect fake keyboards;
- detecting abusive transaction reversal;
- physical measures to prevent money traps;
- a border around the keypad to prevent PIN entry being monitored.

Electronic Security

One of the main objectives of criminals in connection with ATMs is to obtain user data. These used to be stored on a magnetic tape, which was relatively easy to copy and forge. This weakness has been addressed by the introduction of chip-enabled cards called EMV[88] ("How to Combat ATM Crime," 2011). EMV is a global standard based on chip technology in credit and debit cards. The cards have a small microprocessor embedded in them, which provides greater security than traditional magnetic stripe cards (EMVCo, 2014, pp.5-6).

The increased security of EMV cards comes from various mechanisms. Each EMV card is validated before use, thanks to cryptographic keys securely stored on the chip and security certificates encrypted on the card by the issuer at the time of personalisation. Furthermore, the exchanged data is dynamically encrypted at the time of each transaction, meaning that each transaction is unique (EMVCo, 2014, pp. 18-23). Thus, even if the data from an EMV card is stolen, it is not useful for making a fake chip. Furthermore, recording from a chip is much more difficult than from a magnetic stripe, although there have been recent cases of this (shimming). These mechanisms make it almost impossible to create a counterfeit EMV card (MacDonald, 2017).

Attacks have also started to target data connections, with perpetrators trying to obtain data using viruses and other malware. ATMs themselves are at risk from an eSecurity perspective, as quite a few use open source software (thus, more than 85% of abuse occurs on Windows ATMs) and conventional telephone/internet connections to the bank ("How to Combat ATM Crime," 2011). Banks use various systems to monitor ATM activity remotely and systems to remotely detect abnormal transactions (Accenture, 2016, pp.23-25).
The data handled by the ATM during the transaction is encrypted. From its introduction until the beginning of the millennium, this was done using the Data Encryption Standard (hereinafter DES) algorithm developed in the 1970s ("ATM Security and 3DES," n.d.). With the rapid development of computer technology and computing power, this has become insufficient for secure transactions. This led to the development of a new encryption algorithm, 3DES (triple DES), which is

8 EMV was developed in the mid-1990s and stands for Europay, Visa and Mastercard, which are the credit card companies that spearheaded the development and widespread adoption of this chip technology. It is a payment technology that uses a tiny, powerful chip embedded in credit and debit cards to make card transactions more secure (Stripe, 2023).

essentially an improvement on DES. The latter uses a 56-bit key for encryption, while 3DES uses the process three times, resulting in a 168-bit key. This makes encryption slower but much more secure (Sholes, 2002, p.2-3).

Transport of Cash and Valuables

Cash handover is the process of handing over or taking over cash from a secure area (e.g. an ATM vault) into the hands of security staff equipped and trained to do so, and vice versa. The customer shall illuminate the handover point and mark it with a sign reading 'Security - No access during handover of a secure consignment'. This 'extension' of the definition of a secure area provides the basis for the security guard to use all measures and other means in that area during the handover of cash and other valuables (Čas and Božjak, 2023, p.17). The Regulations on the Method of Transport and Security of Cash and Other Items of Value (2016) specify in more detail the method, minimum conditions and security measures for the transfer, transport and security of cash and other items of value, in order to prevent the risk of theft and to ensure the safety of persons transferring, transporting and securing cash and other items of value.

The licensee and the transfer and transport operator shall endeavour to eliminate the hazards arising from the risk assessment of the transfer and transport by taking appropriate measures to mitigate the hazards within their respective spheres of competence.

Security measures include:

- preventive security measures and technical security system;
- escort by security guards;
- combined use of technical security and security escort;
- drawing up a transfer and transport plan and
- police cooperation.

The class of transfer and transport of a secure consignment is determined by adding together all the cash and the value of other items of value being transferred or transported at any one time.

The Regulations thus define several classes of transfers and transport of secure shipments:

- Class 1, the value of which does not exceed € 50,000;

- Class 2, the value of which does not exceed € 200 000;
- Class 3, the value of which does not exceed € 1 500 000;
- Class 4, the value of which does not exceed € 4 000 000 and
- Class 5, the value of which exceeds € 4 000 000.

The handover of Class 1, 2 or 3 secure shipment shall take place at a lighted handover point which, at the time of handover, has the status of a secure area, at a distance which prevents direct physical force being exerted on security staff. If all of the above cannot be ensured, the handover shall be carried out with an additional armed security guard.

The secure handover area shall be equipped with technical security systems capable of monitoring the immediate surroundings of the facility, physically separated from the surrounding area in order to prevent unauthorised persons from entering and viewing the facility, and shall have the status of a secure area at the time of handover. A secure area is considered to be a premises, facility or area owned, leased or managed by the service provider, which is an area designated by contract with the licensee, where internal security is provided and the immediate vicinity of the protected person (Čas, 2023, p.52).

Where a secure handover area cannot be established at border crossing points in the manner described above, the transport contractor may propose the involvement of the police. In carrying out police tasks, police officers decide, based on the circumstances given to them at a given moment, which police power to exercise to prevent and eliminate danger (Pozderec and Kotnik, 2023, p. 17). Police officers are required to respond quickly to different security phenomena when carrying out different forms of police tasks in a given area and time of operation. When acting with police powers[9], police officers establish public order, prevent offences and crimes, apprehend offenders and misdemeanours, and thereby facilitate the processing of offenders (Žaberl, Pozderec, and Oberman, 2017, p.275).

For the transport of a Class 4 or 5 secure shipment, a transport plan must be drawn up in advance, covering the procedures and measures to be taken before collection or handover, during transport and stops,

9 Police powers are legally prescribed measures which enable police officers to effectively and successfully perform their tasks. When performing their tasks, police officers must act in accordance with the Constitution and laws and respect and protect human rights and fundamental freedoms (Ministry of the Interior, 2024).

and the traceability of the transport. The contents of the plan must be communicated to all security staff involved in the transport before the transport takes place. The customer of a transport of a Class 4 or 5 secure shipment may propose the involvement of the police in the transport and security of the secure shipment. In the event of police involvement in the transport and security of the consignment, the licensee and the police shall agree on the form of their cooperation (Regulations on the method of transport and security of cash and other valuable consignments, 2016).

Proposal for Comprehensive ATM Security

The development of ATMs allows users to easily access cash and perform more and more tasks at ATMs. As the number of transactions increases, so do the various forms of abuse of ATMs, which are being developed in order to circumvent the preventive and security measures in place to prevent the commission of a crime by which criminals illegally obtain property. In the case of known forms of ATM abuse, the abuse itself must first be identified and recognised so that it can be prevented or stopped. Certain forms of ATM abuse have been made impossible with the development of the EMV chip and PIN entry. Chip counterfeiting is difficult, but most chip cards still have a magnetic stripe, which poses a potential risk (Security News Desk, 2016).

Different methods of ATM security are used. Axis Communications developed the AXIS P12 series and then the AXIS F network camera series to prevent the rise in ATM abuse. These are flexible, small, adaptable network cameras that can be attached to the ATM. The AXIS F-series has enhanced capabilities to handle a wide range of lighting conditions and four camera versions. In fact, it has a body with four different lenses. In Asia, it is mandatory to have up to four cameras in some areas to protect ATMs. Surveillance of ATMs with cameras allows the link and insight between videos and transaction data in disputes between users and suspicious activities. Honeywell Security has developed the SC 100 motion detection sensor. The sensors detect vibration signatures of different types of abuse at ATMs. They contain detection algorithms that help filter out false sources of triggered alarms (Security News Desk, 2016).

In recent years, banks have shifted to anti-skimming analysis to protect ATMs from abuse. This involves video analysis of complex scenes. The

key is to identify the setting of skimming devices that can be inserted above the card slot. Anti-skimming analysis works in a way that it blends in with objects placed in the background and is not visible to the user. The device also works in the event of blackout. With video analysis, the bank captures images of people using the ATM and receives an alert when someone is standing next to the ATM. Based on the video images integrated with the central transaction server, the bank is able to set up searches for cases where a person is in front of the ATM but not making a transaction. This is an indication that someone may be installing a skimming device. In situations like this, the system triggers an alert and lists the instances in the report that match this description along with other information such as date, time and location. The security officer shall examine the video and the report and, if necessary, inspect and check the ATM for changes to it. In the case where the perpetrator used cards with stolen cardholder data at the ATM, the bank's video surveillance may, as in the previous case, look for persons making multiple withdrawals with different cards. The bank's video surveillance captures images of the person making the ATM transaction. The system compares the transactions with the video recordings and flags cases where the person has stayed at the ATM and made multiple transactions with different cards. The system shall list the transactions found in a report. This allows security authorities to quickly identify cash theft (Cremins, 2015).

The Information Systems Group has developed fingerprinting technology that is used in ATMs in Japan. ATM users use a card and place their finger on the scanner. The reader reads the finger's biometric record and checks it against the stored data on the card. Therefore, PIN is no longer needed. 80 % of ATMs in Japan use this technology (Security News Desk, 2016).

The perpetrators are often one step ahead of the banks and security services, and they are only reacting to new or sophisticated abuse. In any case, more advanced ATM security methods can help to reduce the number of abuses or the damage suffered by users and banks.

Conclusion

ATMs are one of the easiest ways to access cash and can also be used for many banking services. ATMs are often the target of abuse due to different security standards. It is important to remember that ATM security actually starts with the choice of the location itself, which should be chosen wisely, checking known information on the incidence of crime in the chosen area, and selecting the right type of ATM with the right system configuration and security level, and ensuring adequate security.

However, the safe use of ATMs cannot be ensured by simply reviewing existing and known types of abuse. Security measures and prevention options are already in place for these types of abuse. Technological developments must be anticipated in order to anticipate the opportunities they offer for perpetrators to detect and carry out new types of abuse, as they are constantly developing new and unknown ways of doing so. Manufacturers and developers must stay one step ahead of the perpetrators and try to prevent or minimise the possibilities of abuse at ATMs. They need to detect anomalies in common transaction data that indicate signs of ATM abuse. It does not matter whether it is a tried and tested method or a new way of a type of ATM abuse (Geller, 2016).

From the users‘ point of view, it is important to be aware of the different forms of abuse, so that they can identify them more effectively, potentially protecting themselves and others. They can further contribute by following preventive recommendations for safe use of ATMs and, to a certain extent, prevent themselves from becoming victims of ATM abuse.

Newer forms of abuse are often of such a nature that they are difficult or impossible for users to recognise. In these cases, the onus is on banks to protect their assets through prevention, good supervision and action.

In addition to bank preparedness, security services and police will also need to be prepared, as investigating and prosecuting such crimes is likely to require a more detailed knowledge of computer equipment, software, encryption and the risks associated with malware.

References

Accenture, 2016. *ATM Benchmarking Study 2016 and Industry Report.* Available at: https://www.readkong.com/page/atm-benchmarking-study-2016-and-industry-report-accenture-7550883

ATM Depot.com., (n.d.). *ATM Security and 3DES.* Available at: https://atmdepot.com/resources/triple-des-3des-encryption-atms/

ATM Security.com., 2011. *How to Combat ATM Crime.* Available at: http://www.atmsecurity.com/articles/27683-how-to-combat-atm-crime

Bankart, (n.d.). ATM Network Management. Available at: http://www.bankart.si/si/ponudba/upravljanje-mreze-bancnih-avtomatov/

Bank of Slovenia, 2023. Bulletin. Available at: https://bankaslovenije.blob.core.windows.net/publication-files/bil2023_12.pdf

Batiz-Lazo, B., Reid, R. J. K. 2008. *Evidence from the patent record on the development of cash dispensing technology.* In: 2008 IEEE History of Telecommunications Conference (pp. 110-114). IEEE. https://doi.org/10.1109/HISTELCON.2008.4668724.

Bennet, K., 2023. *Automated teller machine: What it is and how to use one.* Available at: https://www.bankrate.com/banking/what-is-an-atm/

Bing, C., 2018. *Cybercrime gang leader who caused ATMs to spit cash is arrested.* Available at: https://cyberscoop.com/carbanak-cybercrime-gang-leader-who-caused-atms-to-spit-cash-is-arrested/

Cremins, D., 2015. *There Really is a Way to Do That.* Available at: https://www.marchnetworks.com/intelligent-ip-video-blog/there-really-is-a-way-to-do-that/

Crossman, P., Ghosh, P., 2017. *How is ATM fraud still a thing? Credit Union Journal.* Available at: https://www.cujournal.com/news/how-is-atm-fraud-still-a-thing

Čas, T., 2023. *Strategic and Developmental View on Private Security in the Republic of Slovenia, with Emphasis on Private Guarding.* 1st ed. Ljubljana: Čas – Private School for Security Education.

Čas, T, Božjak, Ž., 2023. *Training for Obtaining National Vocational Qualification for Security Guard.* 1st ed. Ljubljana.

Diebold, N., 2012. *ATM Fraud and Security.* Available at: https://www.yumpu.com/en/document/read/2355432/atm-fraud-and-security-diebold

Dublino, J., 2024. *Cash Register Buying Guide: POS vs. Cash Registers vs. Tablet mPOS.* Available at https://www.business.com/articles/cash-register-vs-pos-system/

E.A.S.T., (n.d.). *ATM Crime Definitions.* Available at: https://www.association-secure-transactions.eu/industry-information/terminal-fraud-definitions/

E.A.S.T., 2015. *European ATM crime report 2014.* Available at: https://www.association-secure-transactions.eu/files/EAST-ATM-Crime-Report-2014.pdf

E.A.S.T., 2018. *Transaction Reversal Fraud.* Available at: https://www.association-secure-transactions.eu/tag/transaction-reversal-fraud/

EMVCo., 2014. *A Guide to EMV Chip Technology.* Available at: https://www.emvco.com/wp-content/uploads/2022/09/EMV%C2%AE-Chip-At-A-Glance-EMVCo-eBook.pdf

ENISA, 2009. *ATM crime : Overview of the European Situation and Golden Rules on how to avoid it.* Available at: https://www.enisa.europa.eu/publications/archive/atmcrime

Europol, 2017. *27 arrested in successful hit against ATM Black Box attacks.* Available at: https://www.europol.europa.eu/media-press/newsroom/news/27-arrested-in-successful-hit-against-atm-black-box-attacks

Geller, Y., 2016. *ATM fraud: The evolution of an epidemic.* Available at: https://www.atmmarketplace.com/articles/atm-fraud-the-evolution-of-an-epidemic/

Harper, T., 2004. *Timeline: the ATM's history.* Available at: https://www.atmmarketplace.com/news/timeline-the-atms-history/

Hirsh, L., (n.d.). *Importance of ATM Machines in a Small Business.* Available at: https://smallbusiness.chron.com/importance-atm-machines-small-business-63116.html

Huš, M., 2015. *An ATM is Also a Computer.* Available at: https://www.monitor.si/clanek/tudi-bankomat-je-racunalnik/168896/

Infogram, 2024. *Number of ATMs in Slovenia.* Available at: https://infogram.com/stevilo-bankomatov-v-sloveniji-1ho16vo1wlzn84n

Kagan, J., 2023. *What is an ATM and how does it work?* Available at: https://www.investopedia.com/terms/a/atm.asp

Klinar, K., 2006. *Economic Analysis of the Project for Introducing Unified Software for Self-service Banking Machines: Master's Thesis.* Ljubljana: Faculty of Economics. Available at: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=9825

Lake, R., 2022. *ATM Withdrawal Limits: What you need to know.* Available at: https://www.forbes.com/advisor/banking/atm-withdrawal-limits/

Lamberger, I., 2011. *Model for Protecting Electronic Payment Systems Against Abuse: Doctoral Dissertation.* Ljubljana: Faculty of Economics. Available at: http://www.cek.ef.uni-lj.si/doktor/lamberger.pdf

Lamberger, I., Dobovšek, B., Slak, B., 2012. *Abuse of Payment Cards – Perspectives of Card Issuers.* In: Journal of Forensic Science and Criminology, 63(2), 123–135. Available at: https://www.policija.si/images/stories/Publikacije/RKK/PDF/2012/02/RKK2012-02_Lamberger_Dobovsek_Slak_ZlorabePlacilnihKartic.pdf

MacDonald, J., 2017. *The new card skimming is called „shimming."* Available at: from https://www.coursehero.com/file/48613579/CYB-115-research-paperdocx/

McAfee, LLC., 2024. *What Is a Trojan Horse?* Available at: https://www.mcafee.com/learn/trojan-horse/

Miller, A., 2011. *Who invented the ATM machine?* Available at: http://www.atminventor.com/

Ministry of the Interior, 2024. *Police Powers*. Ministry of the Interior, Police, Republic of Slovenia. Available at https://www.policija.si/eng/about-the-police/police-powers

Negg Blogg., 2024. *Cash trapping: the ATM scam.* Available at https://negg.blog/en/cash-trapping-the-atm-scam/

Pozderec, F., Kotnik, K., 2023. *Police Powers with Practical Procedures 1*. Ljubljana: Ministry of the Interior, Police.

Ropret, M., 2017. *NLB Introduces Contactless ATMs and Announces Phone Payments.* Available at: https://tehnozvezdje.si/nlb-uvaja-brezsticne-bankomate-in-napoveduje-placevanje-s-telefoni/

Ropret, M., 2023. *By the End of the Year, More Than 50 ATMs for the Blind and Visually Impaired.* Available at: https://tehnozvezdje.si/do-konca-leta-vec-kot-50-bankomatov-za-slepe-in-slabovidne/

Rules on the Method of Transport and Protection of Cash and Other Valuable Consignments, 2016. Official Journal of the Republic of Slovenia (88/16).

Security News Desk, 2016. *ATM security in the battle against fraud and physical attacks.* Available at: https://www.cybercureme.com/atm-security-in-the-battle-against-fraud-and-physical-attacks/

Sholes, D., 2002. *Triple DES and Encrypting PIN Pad Technology on Triton ATMs.* Available at: http://www.atmdepot.com/wp-content/uploads/2011/03/3DESWP.pdf

Stripe, 2023. *What are EMV chip cards? How EMV works and why it's so secure.* Available at https://stripe.com/en-si/resources/more/what-are-emv-chip-cards#what-is-emv

Weight, A., 2009. *Best practice for physical ATM security. ATM Security Working Group.* Available at: https://www.coursehero.com/file/219327699/Best-practice-for-physical-ATM-securitypdf/

Wieder, N., (n.d.). *ATMs fort he Visually impaired.* Available at: https://atmdepot.com/articles/atms-for-the-visually-impaired/

Združenje bank Slovenije, 2021. *Basic Rules for the Safe Use of ATMs.* Available at: https://www.zbs-giz.si/?s=temeljna+rules+for+safe+use+of+ATMs

Žaberl, M., Pozderec, F., Oberman, I., 2017. *Prevention of Danger as a Basis for the Exercise of Security Powers.* In: Security Studies: A Journal for the Theory and Practice of Security Studies.