ARTICLE:

A case of the customer attempting to claim their debit card was cloned

By **Jerzy Kosiński**

Summary

The author of the paper describes, from the point of view of the bank and the expert, an attempt to steal over 300.000 PLN (75.000 Euro), using the microprocessor (called a chip) in a debit card. The evidence clearly indicated the perpetrator's guilt.

Introduction

Frauds using credit cards are more often associated with acquiring data from a genuine credit card and using the data to make a false card, or making a payment that does not require the physical card. The first option includes the production of a clone card, which can be used identically as the original card. Sometimes criminals trying to extort money from the bank, claiming that their credit card has been cloned.

Background

On 9 February 20XY Leszek Z. called his bank to file a complaint regarding transactions over the period of time between 21 January 20XY and 5 February 20XY. He claimed he did not perform the transactions complained of, and suggested that his card must have been copied. The man stated that the last transaction he performed using his credit card was on 8 February 20XY. In the period of time, when the transactions mentioned in the complaint were performed, he was on vacation and was in possession of his card, but he did not use it. At the same time he demanded return of the funds that were debited – over 300.000 PLN. Leszek Z. informed the bank that he reported the theft to the police. During the telephone call he made, because of the risk that the card could be copied (skimmed), the card was cancelled. The day after, on 10 February 20XY, the victim's credit card was retained by the ATM, when the customer tried to withdraw funds. The ATM owner sent the card retained by the ATM to the bank. The bank started a standard complaint process, which aimed to determine a number of questions:

1. The type of debit card that was involved in transactions regarding the complaint. It was determined that the transactions involved a microprocessor debit card. All of the transactions were performed using data from the microprocessor and required the entering of a PIN.

2. Where the transactions were performed. The bank account of Leszek Z. was checked regarding withdrawals using his debit card. Other issues included establishing date and time, the type of transaction, and the ATM's that were used. The first three transactions were performed on Polish territory, next on German territory, and the remaining on Polish territory.

3. Whether other banks had reports of skimming in ATM's or about this particular card. None of the banks had any information about the existence of such facts.

As a result of the analysis, the bank determined that there were no reasons to accept the complaint, and on 31 March 20XY the bank informed the customer in writing, that it did not accept the complaint was supported by the evidence.

However, because the circumstances of the case were suspicious (the skimming of a microprocessor card) it was adjudged that the standard investigative procedure should be expanded and the case was handed on to Banking Crime Department of Bank Security Bureau (BCD).

Analysis and interpretation of data

The BCD revised the case under three aspects:

1. Inspecting the bank account history of the customer, with particular caution regarding use of the compromised card.

2. Analysis of the chosen mechanics of the actions of the microprocessor in the card.

3. Verification of the authorisation logs.

Bank account history

The account, which operated by the card that the ATM retained, was opened on 24 April 20XY-1 (20XY-1 is the year before the losses) as a company account, and Leszek Z. was appointed as an authorized signatory (Leszek Z. was 36 years old at this time and was running his own company). From this point on the account registered over 1300 operations. The operations were mostly internet transactions (outgoing and incoming transfers) and direct cash deposits (reaching several thousand PLN). On 30 December a Visa Electron debit card was added to the company account. It was a microprocessor card. The daily withdrawal limit was set to 5.000 PLN. Two weeks later (mid January 20XY), the customer applied for an increase in the daily withdrawal limit of up to 20.000 PLN. The card was blocked on 9 February 20XY. There were 66 operations performed using the debit card (cash withdrawals and card payments). Leszek Z. admitted to have performed first three. The next 61 operations were the matter of the complaint, and were performed between 21 January 20XY and 5 February 20XY (the majority of these transactions were withdrawals of cash in ATMs located by petrol (gas) filling stations in Germany). The next two (last recorded) operations were performed by Leszek Z., and on 10 February 20XY the card was retained by the ATM when Leszek Z. attempted to initiate an operation. The ATM, in which the card was retained, was adapted to handling microprocessor cards.

The microprocessor card

The information necessary to perform an operation with a microprocessor card is stored in the memory of the integrated circuit (microprocessor, chip). Nevertheless, to enable the user to use the card on devices that cannot read such information from the microprocessor, the magnetic stripe remains on the card. If the machine that reads the card (e.g. ATM or POS terminal) is adapted to microprocessor cards, then the data are always collected from the microprocessor memory, not from the magnetic stripe. One of the elements of microprocessor memory is called ATC registry (Application Transaction Counter), often called the 'transaction counter'. The card given to the customer has the counter of the registry set to 0 (zero). Every transaction (or an attempt) that is performed in a device adapted of reading the data on the microprocessor increases the registry value by 1 (one).[1]

Analysis of the authorisation logs

Each time an operation is performed using a debit card, the software sends an authorisation packet to the bank, which contains the following data: transaction details, card data, PIN, etc. A card with a microprocessor that is used in devices adapted to reading such cards, the authorisation packet also includes the actual value of the 'transaction counter' (ATC), which is read from the microprocessor. If the operation is performed on a device that is not adapted to microprocessor cards, the data are read from the magnetic stripe. In such a case, the ATC registry value sent to the bank is 0 (zero). The authorisation packets are stored in authorisation logs. The authorisation logs in the computer system of the bank regarding the debit card in question demonstrated that the ATC chronology was correct. For the first operation on the device adapted to microprocessor cards, the value of the ATC registry was set to 1. For the last transaction, the value of the ATC registry shown at 72. With 66 operations performed, there may be gaps (jumps) in the ATC registry numeration in the authorisation logs. If this is the case, it means that the authorisation centre of the bank has not received the data of the transaction (authorisation packet). This can occur because of a number of reasons. Some of the reasons include: the customer cancelling the operation; recalling the operation in an ATM, or the device is not able to reach the bank's authorisation centre. Such examples are perfectly normal. The last transaction before the matter complained of and not questioned by the customer, was performed on 11 January 20XY in a device adapted to reading a microprocessor and had set the number of the ATC registry to 3. All of the operations that were challenged by the customer were performed on devices adapted to reading microprocessor – the first of these (21 January 20XY) set the counter to value 4, the last (5 February 20XY) set the ATC registry to the next, bigger by 1 value = 70. On 10 February the card was retained by the ATM, which set the counter to 72.

[1] For a detailed description of how this works in English, see Stephen Mason, *When Bank Systems Fail Debit cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong* (2nd edn, PP Publishing, 2014).

As a result of this further analysis, the BCD had to consider indirect proof.

Let us suppose that Leszek Z. told the truth, and his microprocessor card was skimmed (copied with full microprocessor content).[2] Keep in mind, that all the operations questioned were performed on devices adapted to microprocessor cards, so the ATC registry in microprocessor was each time increased by 1 (one):

1. On 11 January Leszek Z. performed an operation on a device adapted to read the microprocessor. The ATC registry on the original card was set to 3 (at this point of time or before the card had to be copied [cloned])

2. On 21 January the first operation with the clone of the card was performed. The ATC registry of the card used will be set to 4 (or at least 2, if the card was cloned during the first operation)

3. On 5 February the last contested operation (61) was performed with the copied card. The ATC registry of the cloned card will be at value at least 63 (if there were only operations dealing with cash withdrawals or payments). The ATC registry value will be higher, if, for instance, there have been unsuccessful withdrawal attempts.

4. On 10 February Leszek Z. tried to perform an operation with the original card in ATM adapted to reading microprocessor. The card had been retained in the ATM and was handed to the bank. The ATC registry of the original card was set after this operation to 72.

However, Leszek Z. claimed that the operations in question were performed with the clone of the original card, then the card retained on 10 February in the ATM, so the original card (which he claimed to have been in possession of during his winter holidays, i.e. during the time the operations in dispute were performed) should have the ATC registry set to a value of 4, because the last operation from 11 January performed by Leszek Z. set the ATC registry of the original card to value 3. However, the authorisation log of the card after it was recovered showed it to have a value of 72, so the assumption that the card was copied is false.

It is therefore concluded that all of the operations were performed with the original card, and not a copy (clone).

On 8 April 20XY, BCD issued a notice to the Regional Prosecutor’s Office setting out a valid suspicion that Leszek Z. committed a crime of fraud of over 300.000 PLN.

Procedural actions

The Regional Prosecutor acquainted himself of the facts of the case concerning financial fraud. The facts for the investigation comprised the withdrawal of cash by using a debit card in the period from 21 January to 5 February 20XY in ATMs on Polish and German territory detrimental to bank. An investigation was initiated under the provisions of art. 286 § 1 Polish Penal Code. A computer crime and debit card witness was asked to give evidence on the following: an inspection of the bank’s computer system; inspecting an experiment involving the use of a microprocessor debit card and determining as an object how the system registers such transactions, and the provision of a expert witness statement on the following issues:

(i) The type of transactions conducted from 21 January 21 20XY to 5 February 20XY;

(ii) Whether it used card Visa Electron no. 40xx xxxx xxxx xxxx;

(iii) The type of devices used to perform the transactions;

(iv) Whether the subject transaction registered in the bank computer system and on the card;

(v) The types of data regarding transaction the bank records, and whether there is amongst those data the ATC registry value of microprocessor card transactions;

(vi) Whether these data matched the records in banking system;

(vii) How verification was carried out on the card when used in a.m. transactions;

(viii) Whether the transactions in dispute were possible without knowledge of the PIN;

[2] As in the case of Bernt Petter Jørgensen, where the bank consistently called him a liar until it was discovered, after two hearings, that he was telling the truth, for which see Maryke Silalahi Nuth, ‘Unauthorized use of bank cards with or without the PIN: a lost case for the customer?’, 9 *Digital Evidence and Electronic Signature Law Review* (2012), 95 – 101.

(ix) Whether the transactions pointed out by the bank in the attachment to the notice about the suspicion of committing a crime dated 08.04.20XY matched the transactions registered by computer system of the bank;

(x) Whether the transactions carried out using a copy of this Visa Electron card, which was retained in the ATM from Leszek Z., or may have been carried using a forged (cloned) card.

Actions of the expert witness

On 3 July 20XY the expert witness visited the headquarters of the bank to inspect the bank's computer system, to review the evidence relating to the data recorded for each transaction performed with the microprocessor card in the system, including the type of data for each transaction with the debit card registered with the system, and on the card with the possibility of establishing whether any of the data in the system and on the debit card was modified. The experiment was carried out involving the use of the microprocessor debit card to determine how the system registered such transactions. During the experiment, besides the expert witness, representatives from the Security Bureau of the bank and from the operating personnel responsible for debit cards of the bank too part. As a result of the inspection, the expert witness stated that the microprocessor debit card transactions are operated using a computer transaction system called Altamira, made by the Spanish company Alnova (bought from Andersen Consulting). The Altamira system is based on the use of a central host – mainframe IBM and database – DB2. The section responsible for providing resources to the bank's customers is based on Microsoft technologies. The security of the system was provided by the following: Resource Access Control Facility (RAFC); Hardware Security Module (HSM) – a hardware module designed to register cryptographic keys and perform cryptographic operations; an Application Programming Interface (API) system, enabling the use of the same software interface during access to cryptographic resources, a Security Resource Manager (SRM).

Cryptographic methods provide for the confidentiality and integrity of the data from transactions received by the bank from terminals, including ATMs. The integrity of the data was controlled by the transaction system. There was no possibility of modifying transaction data manually that would not be recorded. The system created daily copies of the security data. The security data are stored for 10 years. The debit card history is available for at least 5 years. The logs of the debit card history in the computer system were inspected and were identical to the logs contained in the other devices.

The main components of the safety features on the microprocessor on the debit card transaction are (i) an obligatory verification (authorisation) of the transaction with the PIN, which helps to prevent lost, stolen, and 'not received' items in regard to card fraud and (ii) there is no possibility of interfering with the data of the information contained on microprocessor by unauthorized individuals. There are no known cases of copying all the data from one microprocessor debit card to another microprocessor debit card.[3]

For the data stored on the electronic card to be compliant with EMV standard, it may be categorized into one of following categories:[4]

(i) information regarding the card owner,

(ii) information regarding the card issuer,

(iii) information regarding security,

(iv) information regarding risk management,

(v) information regarding transaction operation.

In the category of risk management (iv), data is mostly used only by the card operating system, however this data may also be read by the terminal (GET DATA function), and additionally, some of the data may be altered during an on-line connection with a bank server (SCRIPT PROCESSING). Which part of this category of data might be altered depends on the particular implementation of the card operation system by the bank, and is not the subject of the EMV standard. Data in this category, called CRM (Card Risk Management), includes:

(i) The transaction counter, known as the Application Transaction Counter (ATC), the main purpose of the ATC registry is to stop 'replay' type attacks. This is where a valid data transmission is repeated or delayed for

[3] Steven J. Murdoch, Saar Drimer, Ross Anderson and Mike Bond, 'Chip and PIN is Broken', in *Proceedings 2010 IEEE Symposium on Security and Privacy* (IEEE Computer Society, 2010), 433.

[4] EMV '96 Integrated Circuit Card Application Specification for Payment Systems (Version 3.0, June 30, 1996 Europay International S.A., MasterCard International Incorporated and Visa International Service Association).

fraudulent purposes. For instance, if the card issuer receives an Application Request Cryptogram (ARQC) and all the data (including the ATC) are the same as previously received by the ARQC, which means the transaction is replayed.

(ii) The value of last ATC, for which the transactions was performed on-line, called Last Online Application Transaction Counter (LATC).

From the point of view of this case, the transaction counter (ATC), using the card application, counts all the transactions performed using the card on devices adapted to reading the microprocessor on the card. The ATC registry is increased in when the GET PROCESSING OPTIONS command is successful, i.e. after inputting the PIN c and it is verified positively. Standard card software does not allow a reset (clearing, zeroing) of the ATC registry. The ATC registry is stored in the ‘data object’ region of the card at address 0x9F36. The Last Online ATC registry value is also stored in the ‘data object’ region at address 0x9F13. The registry from this address is set to the ATC value equivalent to the last transaction, which was sent on-line to authorisation. A card meeting the EMV standard has the GET DATA command implemented. Using this command, the terminal will receive (read) both ATC values. The terminal may calculate the number of off-line transactions as the difference between the values of the ATC registry and the Last Online ATC registry. In the case of the microprocessor debit cards issued by the bank, the ATC registry cannot be altered using software on the transaction operation system level. The system only records the ATC registry value sent by terminal (ATM, POS). During the personalization of the card, the card producer may set this value (this function is also used during personalization of a duplicate card).

To perform the first part of the experiment, the microprocessor debit card was used, Visa Electron no. 40xx xxxx xxxx xxxx, called ‘card1’ and a Euronet[5] ATM that was adapted to reading microprocessor debit cards. An inspection of card1’s history in the computer system determined that the current ATC registry value was 40. Card1 was put into the ATM and the 50 PLN cash withdrawal option was selected. When the transaction was finalised, the option to print the transaction receipt was selected. The bank’s computer system was checked upon return to the bank headquarters. There was a transaction logged with following data (the data set out below is the only data that is significant for the case):

Type of operation:	CASH WITHDRAWAL IN ATM
Date and time:	XY.07.03 11:15
ATC registry:	41
Type of transaction/confirmation:	CHIP-FULL
Response status:	OK
Amount:	50
City:	street v city z

The following data corresponded with the information on the transaction receipt: type of operation, date and time, amount, city. The ATC registry was increased by 1, so it had a new value of 41. The response status results from accepting the transaction (OK) and increasing the ATC registry. The type of transaction indicated that the transaction was performed using the microprocessor and was confirmed by imputing the PIN.

The second part of the experiment occurred at 11:18, and consisted of inputting card1 to the ATM and selecting the 50 PLN cash withdrawal option, and then cancelling the transaction. The computer system did not record the cancelled transaction.

[5] Euronet Polska Sp. z o.o. is a part of Euronet Worldwide, http://euronet.pl/start.html.

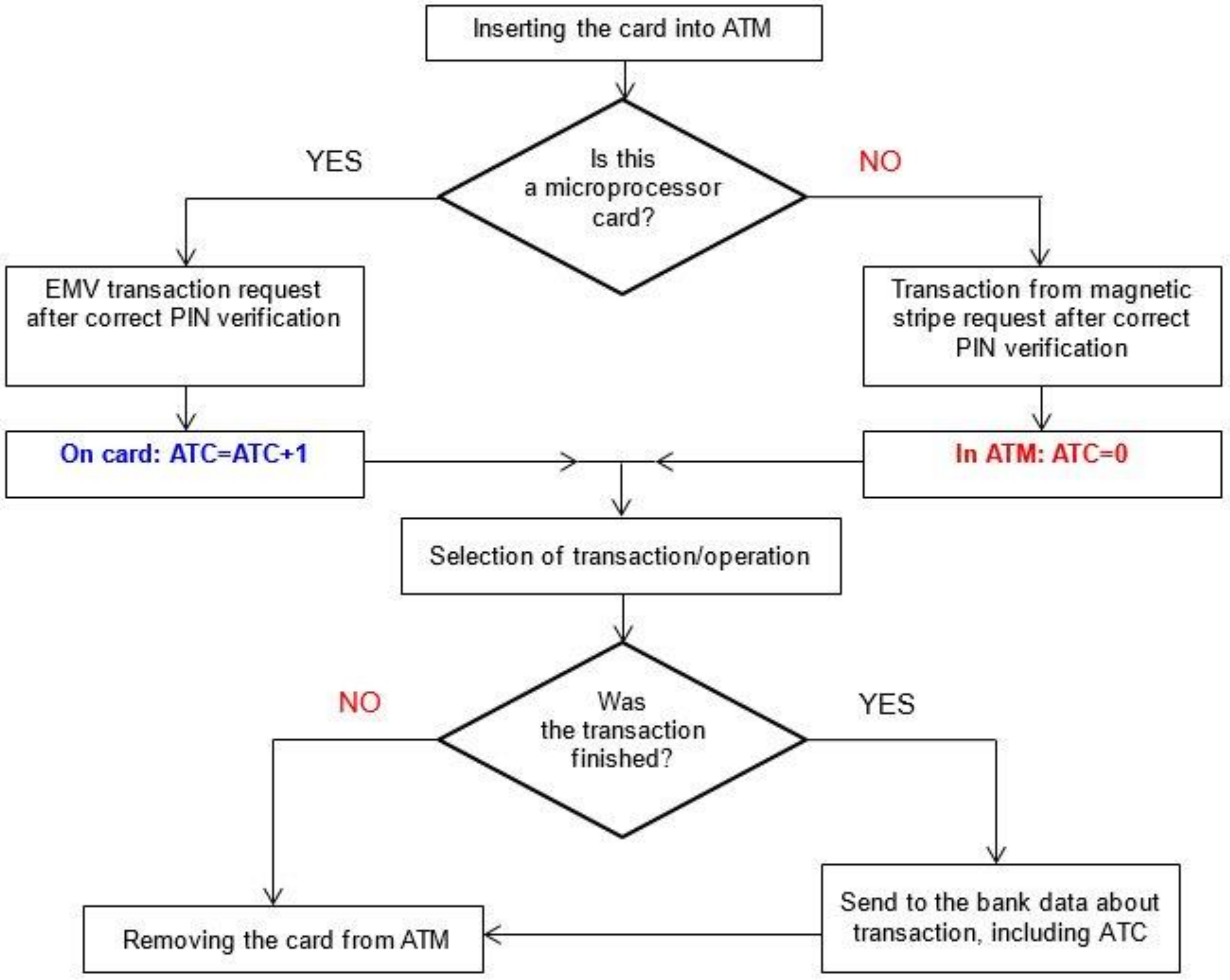
Inserting the card into ATM
Is this a microprocessor card?
YES
NO
EMV transaction request after correct PIN verification
Transaction from magnetic stripe request after correct PIN verification
On card: ATC=ATC+1
In ATM: ATC=0
Selection of transaction/operation
Was the transaction finished?
NO
YES
Send to the bank data about transaction, including ATC
Removing the card from ATM

Figure 1: Process of the on-line transaction in the ATM (please pay attention to the ATC registry)

The third part of the experiment occurred at 11:18, and consisted of inputting card1 to the ATM and selecting the 50 PLN cash withdrawal option, then finalizing the transaction, and accepting the option to print the transaction receipt. The bank's computer system logged the following data:

Type of operation:	CASH WITHDRAWAL IN ATM
Date and time:	XY.07.03 11:18
ATC registry:	43
Type of transaction/confirmation:	CHIP-FULL
Response status:	OK
Amount:	50
City:	street v city z

The following data corresponded with the information on the transaction receipt: type of operation, date and time, amount, city. The ATC registry showed a value higher by 2, which is the result of increasing the ATC registry counter after authentication during the cancelled transaction (second part of the experiment) and increasing its value by 1 as a result of the transaction (third part). The response status is a result of accepting the transaction (OK). The type of transaction indicates that the transaction was performed using the microprocessor and was confirmed by imputing the PIN.

In the last part of the experiment an ATM was used, which read the debit card's data from the magnetic stripe, not from the card's microprocessor. The card1 was once more input into the ATM, and the 50 PLN cash withdrawal option was selected, and in finalizing transaction, the option to print the transaction receipt was selected. The bank's computer system logged the following data:

Type of operation:	CASH WITHDRAWAL IN ATM
Date and time:	XY.07.03 12:17
ATC registry:	0
Type of transaction/confirmation:	FALLBACK-NN
Response status:	OK – FALLBACK TRANSACTION ALLOWED
Amount:	50
City:	street v city z

The following data corresponded with the information on the transaction receipt: type of operation, date and time, amount, city. The ATC registry sent to the computer system showed value 0, which is the result of processing card without the microprocessor (or where the microprocessor is damaged), but with the functional magnetic stripe. The response status is a result of accepting transaction (OK) performed using magnetic stripe (FALLBACK). The type of the transaction indicates that it was done using magnetic stripe (FALLBACK). The previous transaction method was not compared (NN), and it was confirmed by inputting the PIN. To check the ATC registry status, one more transaction was done in an ATM adapted to reading microprocessor debit cards. Card1 was input into an ATM, the 50 PLN cash withdrawal option was selected, and the transaction was finalized. The bank's computer system logged the following data:

Type of operation:	CASH WITHDRAWAL IN ATM
Date and time:	XY.07.03 12:48
ATC registry:	44
Type of transaction/confirmation:	CHIP-FULL
Response status:	OK
Amount:	50
City:	street v city z

Following this inspection and the experiment, the expert answered the prosecutor’s questions. The expert witness concluded that in the period of time from 21 January to 5 February 20XY, using Visa Electron no. 40xx xxxx xxxx xxxx, there were 51 cash withdrawals performed in an ATM abroad (Germany), 9 withdrawals in Poland and once balance check was performed. All the transactions performed in Poland were carried out in one place – Chojnowo. The transactions carried out in Germany took place in 7 locations. All 61 transactions were performed in ATMs meeting the EMV standard – ATMs carrying out transactions based on the card’s microprocessor data. All of the transactions were recorded in the bank’s computer system, and the records in the computer system were identical to records to those contained in the acts of the case. The microprocessor registry and counters could not be read from the actual debit card due to it being blocked. The ATC registry value, of the card retained by the ATM during its last transaction and logged in the bank’s computer system had a value of 72. The bank’s computer system logged transactions include following data (example values), which was sent by the terminal:

Card number:	40xxxxxxxxxxxxxx
Type of operation:	CASH WITHDRAWAL IN ATM
Date and time:	XY.07.03 12:48
ATC registry:	44
Type of transaction/confirmation:	CHIP-FULL / PIN code
Response status:	(000) correct
Amount:	2346.63
Country code:	DE
City:	HILDESHEIM
Terminal type:	ATM
Acquirer’s BIN:	414299
Acquirer:	B+S Card Service GMBH (authorisation centre)
Terminal’s ID:	00000188
Merchant:	REISEB HILDESHEIM-HBF or Market 18/19 (acceptant)
Cryptogram:	OK (confirmation of correct transmission encryption)

Amongst the data sent to the banking system, the ATC registry performed with the microprocessor card. All the transactions that took place between 21 January to 5 February 20XY with the customer’s card could not have been undertaken without knowledge the verification of the card, which consisted of checking the PIN. The bank transactions logs raised the suspicion that a crime was committed using Visa Electron no. 40xx xxxx xxxx xxxx. Assuming the customer’s card was cloned (that is, a new forged card was created, it being a true copy of customer’s card in the moment of cloning – at least regarding the data used to operate the electronic transactions) and withdrawals in the ATM were performed using a copy, each EMV transaction – and it is the case regarding the transactions that were questioned – increased by 1 in the ATC registry on the cloned card. The ATC registry on the cloned card, according to transaction log in the banking system, should show a value of at least 64 (ATC>=64). On the evidential card (that is, the original card), the ATC registry should have remained the same if it was cloned. There had been only one such EMV transaction performed and registered during this time (and one transaction carried out using the magnetic stripe, which does not alter the ATC registry value). During the last transaction of the original card, the ATC registry value shown was 72. If the transactions in question were carried out with a cloned card, then the read counter value should have shown an ATC value of 4. Alternatively, assuming that the user of the original card cancelled any EMV transactions, then taking into consideration the claimed lack of use of the card by the customer, it should show a higher value, but not as many as 72. In the case of transactions performed using a microprocessor, the modification of the ATC registry always occurs on the card, which was physically used to perform the transaction. There is no possibility of a simultaneous, synchronic increase of the ATC registry value on the original card in conjunction with use of a cloned card (keep in mind, there are no known cases of successful, full microprocessor card copying) or vice versa.

Conclusions

The final conclusion of the expert witness confirmed the BCD finding – to perform the transactions in question, the original card must have been used. In the facts described in this case, there are no other technical possibilities that can offer an alternative explanation. The tests confirmed that the original card was used, and at the same time, the evidence indicates that the perpetrator tried to claim they lost over 300.000 PLN to the bank's detriment.

By inspecting the telephone call history of the customer, correlating it with the card transactions log, and inspecting the logging of the SIM to mobile relay stations and to people with whom he contacted, could provide more relevant information. Inspecting the ATM monitoring recordings, where available, could also provide an image of the person(s) performing the withdrawals. Nevertheless, this case is an example that not all offenders are well prepared to hide their actions. The court decided to admit the findings of the expert witness and sentenced the defendant to imprisonment.

Jerzy Kosiński is a Lt. Col. and associate professor of Engineering at the Institute for Research on Crime and Terrorism, Police Academy in Szczytno, Poland, specializing in cyber crime and digital evidence. He has organized a series of international conferences on *Technical aspects of ICT crime* and *Electronic payment instruments abuses*.

kosinski@wspol.edu.pl