#SafeCard: Ukraine's answer to cyberthreats targeting cardholders

Received (in revised form): 2nd February, 2018

Olesya Danylchenko

is deputy director, head of payment instruments and credits security forum for the Ukrainian Interbank Payment Systems Members Association (EMA). She has 17 years' experience in payment cards and ATM risk management, security and fraud prevention, with seven years specialising in payment cards and ATM interbank antifraud information exchange, and private and public sector cooperation in Ukraine. She started her professional career in 2000 as a risk manager at Interbank Processing Centre Topaz of the National Bank of Ukraine after graduating from the Cybernetics Department of Kiev State University. In 2001, she was invited by the security department of JSCB Ukrsotsbank to develop strategies and implement security rules and procedures for bank in-house processing, payment card and ATM fraud prevention and monitoring. While in this post, in 2007 she obtained an MBA specialising in strategic management. In 2010, she joined EMA as head of payment instruments and credits security forum, where her remit covers improved cooperation, and exchanging incidents and experience between financial institutions and law enforcement agencies of Ukraine and neighbouring countries. Since 2011 she has represented Ukraine in the European Association for Secure Transaction (EAST) and since 2016 has been a member of the Advisory Group on Financial Services (AGFS) of EC3 (European Cyber Crime Centre) Europol.

Deputy Director, Head of Payment Instruments and Credits Security Forum, Ukrainian Interbank Payment Systems Members Association (EMA), Office 177, Floor 15, Entrance 5(1), 2B Mykilsko-Slobidska str., Kiev, Ukraine, 02002
Tel: +380 95 4262354; E-mail: oda@ema.com.ua

Abstract This paper reviews the project #SafeCard that was implemented by the Ukrainian Interbank Payment Systems Members Association (EMA) with the financial support of the US Embassy in Ukraine. The project spanned 2016–17 in Ukraine. Its aim was to minimise the level of fraud of payment instruments and ATMs. A number of political and economic factors in Ukraine have contributed to a significant growth in cybercrime schemes targeting bank clients. The main threat to Ukrainian cardholders is the use of social engineering methods that aim to complete operations in a card-not-present (CNP) environment (voice phishing (vishing), SMS phishing (smishing) and phishing websites), along with skimming and cash trapping in ATMs. Threat analysis and forecast was conducted, a common vision for the future was agreed and the following main objectives were determined: 1) To improve Ukraine's criminal legislation; 2) To raise awareness among Ukrainian citizens; 3) To improve capacities of criminal justice professionals to obtain and check information in banks; 4) To improve the knowledge and skills of criminal justice professionals and their cooperation with banks; 5) To raise awareness among prosecutors and judges. This was the first implementation of a project on this scale in Ukraine. As well as meeting the desired challenges, the project also resulted in a hugely positive experience and strengthened the synergy of public–private partnerships. This paper describes the project and the final results. The author hopes that readers will gain some insights that will be beneficial for work to prevent payment fraud in their own countries.

KEYWORDS: Ukraine, vishing, smishing, phishing, awareness, cooperation

ABOUT EMA

The Ukrainian Interbank Payment Systems Members Association (EMA) has been working since 1999 to create favourable conditions in Ukraine for the development of secure and convenient cashless payments and services. This includes implementation and administration of the Ukrainian online system of interbank, international and interagency sharing of information on incidents of payment and ATM fraud, 'Exchange-online'. This capability makes it possible to analyse and process the latest information about crimes related to payment instruments and ATMs, the problems that arise during investigation and bringing the perpetrators to criminal responsibility, as well as providing accurate data about payment fraud trends in Ukraine.

EMA has been coordinating the activities of banks and financial companies since 2001 to counter fraud related to payment instruments and ATMs, successfully collaborating with the cyber police department (CPD) of the National Police of Ukraine, the European Association for Secure Transaction (EAST) and the European Cyber Crime Centre (EC3) Europol.

PROJECT BACKGROUND

Ukraine took the first steps in the fight against payment instruments and ATM fraud in 2001 with the specialised Article 200 'Illegal Actions of Remittance Documents, Payment Cards and Other Means of Access to Bank Accounts, Equipment for Their Production' in the Criminal Code of Ukraine, and the creation in 2006 of a specialised unit within the Interior Ministry to combat crimes in the field of high technology. Ukraine remains very attractive to financial cybercriminals.

Intensive introduction of innovative payment instruments and services, decriminalisation of Article 200 of the Criminal Code of Ukraine, rising unemployment, reduced welfare for citizens and migration processes in the country have led to an increase in financial cybercrime that is no longer just a threat to financial institutions alone (see Figure 1). Since 2014 cybercriminals have chosen as their victims the citizens of Ukraine. They have concentrated their efforts on the most unprotected and trustful categories: immigrants and citizens of Ukraine's Anti-Terroristic Operation (ATO) Zone, new mothers, pensioners and poor families.

The main threat targeting Ukrainian cardholders is the use of social engeneering methods that aim to complete operations in a card-not-present (CNP) environment (see Figure 2).

Vishing: voice communication between criminals and victims with the aim of

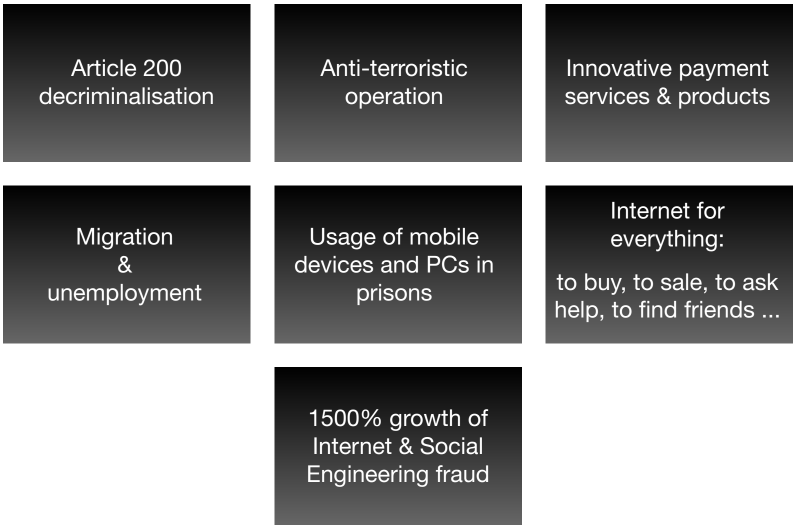
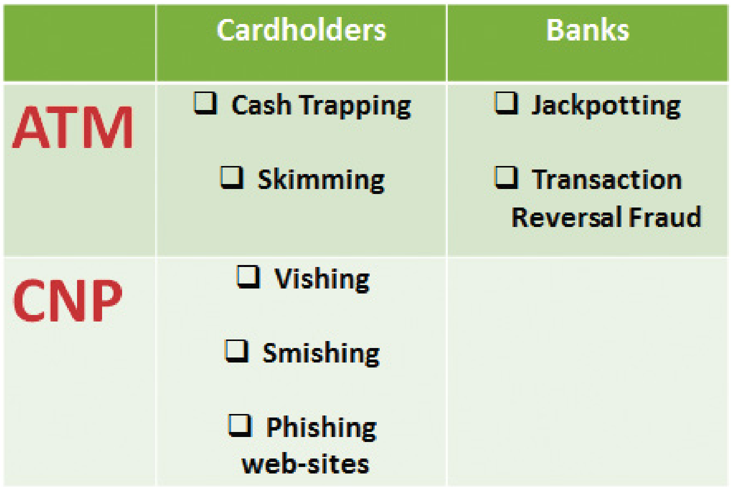

Article 200 decriminalisation
Anti-terroristic operation
Innovative payment services & products
Migration & unemployment
Usage of mobile devices and PCs in prisons
Internet for everything:
to buy, to sale, to ask help, to find friends ...
1500% growth of Internet & Social Engineering fraud

Figure 1: Ukraine today
Source: EMA



	Cardholders	Banks
ATM	□ Cash Trapping □ Skimming	□ Jackpotting □ Transaction Reversal Fraud
CNP	□ Vishing □ Smishing □ Phishing web-sites	

Figure 2: Main fraud trends in Ukraine
Source: EMA

obtaining card data, including the online transaction password (OTP) sent by banks via SMS, in order to complete fraudulent transactions in a CNP environment; and/or to obtain personal data so as to pass victims' identity checks in bank call centres for the purpose of changing security parameters to complete operations in a CNP environment on larger amounts; and/or to persuade victims themselves to complete card-to-card (C2C) or person-to-person (P2P) payments to criminals' own cards and accounts.

Smishing: criminals send SMS to victims with the message that their cards have been blocked by the bank or that they have won a prize (car, apartment, etc.). Victims are requested to call a number and the criminals continue their work via a vishing scenario.

Phishing websites: fake websites that simulate legitimate payment services to complete C2C payments or payments for vehicular communication. These websites have professional SEO support, meaning their SEO score is higher than that of many legitimate payment services, thereby placing them higher on Internet search results. These fake sites also use simple and reliable social engineering methods (usage words) to attract victims' attention: 'first payment without commission', 'zero commission', 'free of commission', etc. Victims who have visited such sites leave the card data necessary for operation in a CNP environment, enabling fraudulent transactions on genuine payment services. Stolen funds are converted into cash via a chain of transactions, including mobile operator services for cash-out, and finally money mules complete cash withdrawals from ATMs. The estimated profit of criminals who work on these schemes increased by 200 per cent over the period 2015–2016 and exceeded 10m Euro.

Victims seek justice by going to the police, but the awareness of law enforcement agency (LEA) employees about the new payment instruments and technologies, along with their knowledge of current fraud schemes, diverges significantly from the level of training of cybercriminals. This awareness and knowledge is significantly reduced with each subsequent stage of the investigation, from operational staff to judges. In Ukraine there is no effective tool for the dissemination of professional information about current financial cyberthreats between all sectors of the criminal process, which significantly reduces the effectiveness of investigations and the possibility of criminal prosecution of financial cybercriminals.

The latest fraud trends are not the only factor determining conditions to implement a comprehensive project on combating fraud via payment instruments and ATMs in Ukraine. Reforms currently in progress at the Ministry of Internal Affairs of Ukraine include a rethinking of the role and purpose of departmental learning systems. Until now there has been no uniform approach to teaching students and retraining existing employees, with multiple independently operated educational institutions offering different curricula. Investing resources in this direction will yield more tangible results following the establishment of a centralised Unified Police Academy and the formation of a specialised unit, acting in close cooperation with specialised non-governmental organisations.

A concentration of activities on restructured the subunits of patrol police and cyber police, which have already demonstrated their leadership and received public confidence and support, will maximise the effectiveness of their partnership with the private sector (banks), and will guarantee continuous improvement of implemented public–private initiatives to counteract crimes involving payment instruments and ATMs.

This was the background to the pan-Ukrainian project 'Counteraction of Payment Instruments and ATM Fraud in Ukraine' (#Safecard), conducted by EMA with financial support from INL Department of the US Embassy in Ukraine.

The project was planned for 12 months and was conducted between October 2016 and September 2017, with the following objectives (see Figure 3):

1. To improve criminal legislation of Ukraine to make it compliant with international standards and adequately address cybercrime related to ATM and payment instruments fraud;
2. To raise awareness of Ukrainian citizens about safe behaviour when using ATMs and payment instruments, and how to prevent, detect and report ATM and payment instruments fraud;
3. To improve capacities of criminal justice professionals to obtain and check information when dealing with criminal proceedings related to ATM and payment instruments fraud;
4. To improve knowledge and skills of criminal justice professionals and their cooperation with banks dealing with criminal proceedings related to ATM and payment instruments fraud;
5. To raise awareness of prosecutors

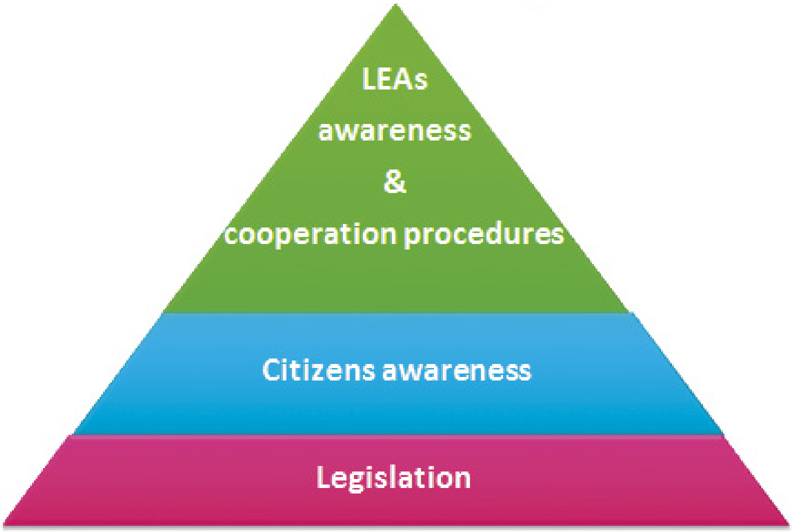


Figure 3: What to change?
Source: EMA

and judges in problematic issues of qualification and criminal proceedings of ATMs and payment instruments crimes.

Based on these objectives, the following project structure was established (see Figure 4). Each objective has a dedicated officer responsible for their component of the project. One large project was divided into five smaller ones.

The proposal was submitted to the US Embassy and received financial support of $198,550 to complete the project, divided between the various objectives (see Figure 5).

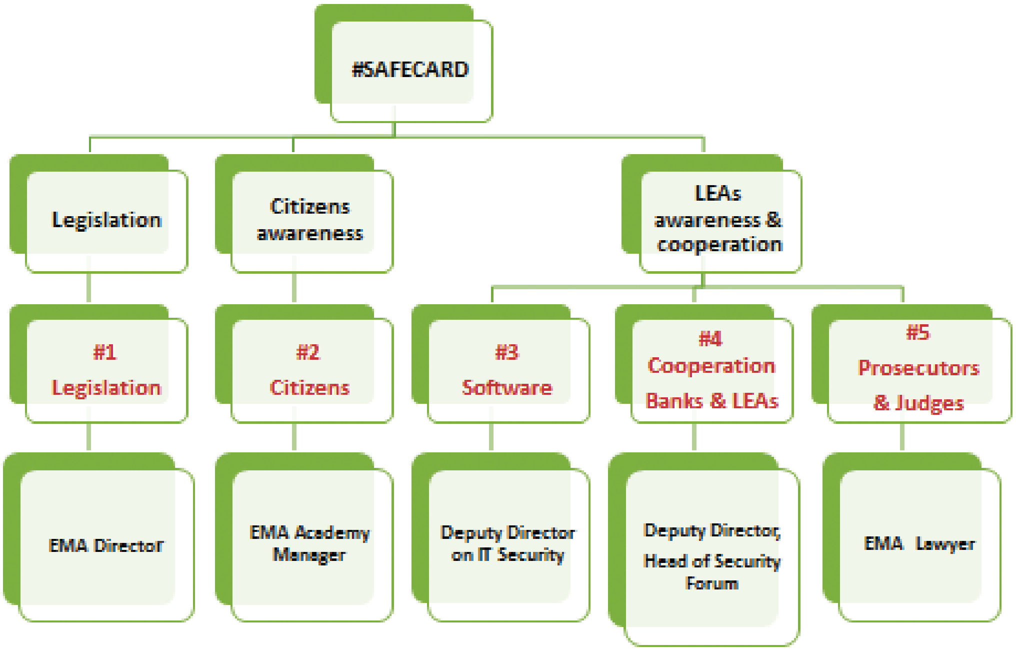


Figure 4: Project structure
Source: EMA

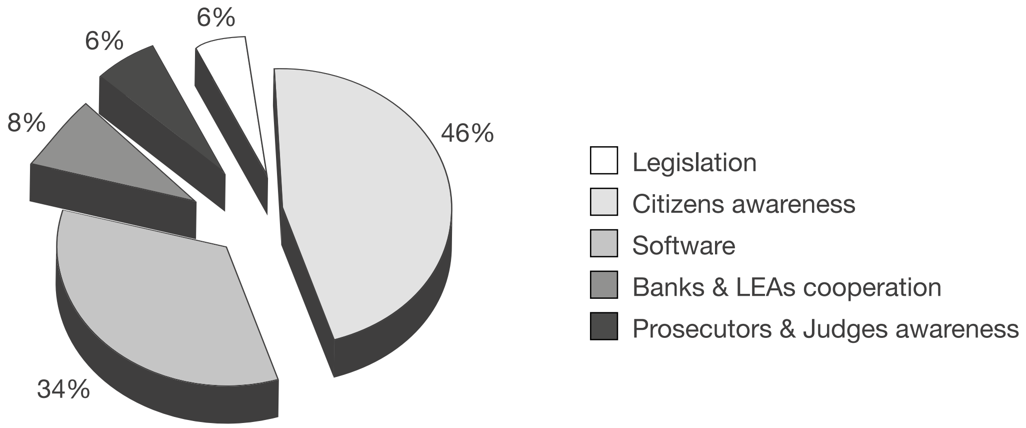


Figure 5: Project budget $198,550, % of budget amount
Source: EMA

The first objective of the project was to improve the criminal legislation of Ukraine to make it compliant with international standards and adequately address cybercrime related to ATM and payment instruments fraud (see Figure 6).

Before addressing the existing criminal legislation of Ukraine concerning responsibility for crimes related to payment cards and ATMs, a comparative analysis of the Criminal Code of the EU member states, fraud trend analysis with payment instruments and ATMs in Ukraine and worldwide was conducted.

The following conclusions were reached:

- Ukrainian legislation does not provide criminal liability for several modern crimes relating to payment cards such as vishing, smishing and phishing;
- Terms of criminal liability stipulated by the legislation of Ukraine for the crimes related to payment cards are considerably low compared to accepted international standards;
- There is a lack of understanding, within the legislature and society in general, that decriminalisation of Article 200 of the Criminal Code of Ukraine 'Illegal Actions of Remittance Documents, Payment Cards and Other Means of Access to Bank Accounts, Equipment for Their Production' contributed to raising the level of payment card and ATM fraud, and that strengthening criminal responsibility, on the contrary, will lead to a decrease.

During project implementation, project officer #1 responsible for this component of the project has achieved the following tasks:

- Elaborated text of the draft law, including amendments to Article 200 of the Criminal Code of Ukraine and agreed it with the National Bank of Ukraine and law enforcement authorities;
- Conducted promotion activities for the draft law in the Banking Committee of the Parliament of Ukraine;
- Received supportive letters from organisations interested in draft law registration;
- The media published more than 40 articles in support of the social importance of the adoption of the draft law by the Parliament of Ukraine;
- The draft law 5361 was registered in the Parliament of Ukraine, passed first reading and recurring first reading.

The result was that the necessary legislative and informational basis for the adoption of

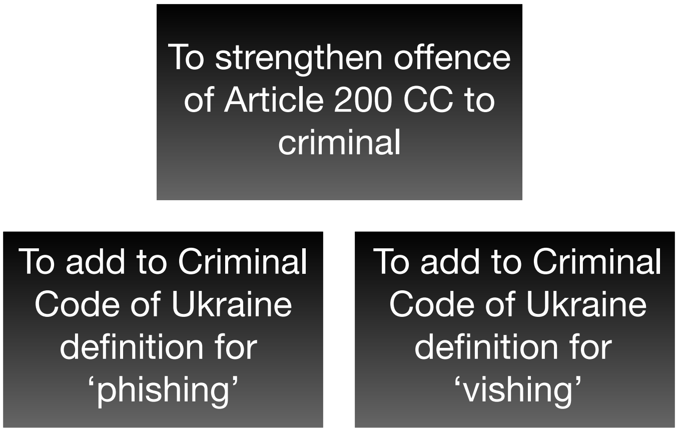

To strengthen offence of Article 200 CC to criminal
To add to Criminal Code of Ukraine definition for 'phishing'
To add to Criminal Code of Ukraine definition for 'vishing'

Figure 6: Project component #1: Legislation
Source: EMA

the draft law by the Parliament of Ukraine was formed. Unfortunately, it did not find enough support in Parliament during the second reading in June 2017, but the background and reasoning behind the desired changes were established. EMA is now working with the National Bank of Ukraine to register another draft law that will have a better chance of passing through Parliament to reach the final goal of legislation improvement.

The second objective of the project was to raise awareness among Ukrainian citizens about safe behaviour when using ATMs and payment cards, and how to prevent, detect and report ATM and payment card fraud (see Figure 7).

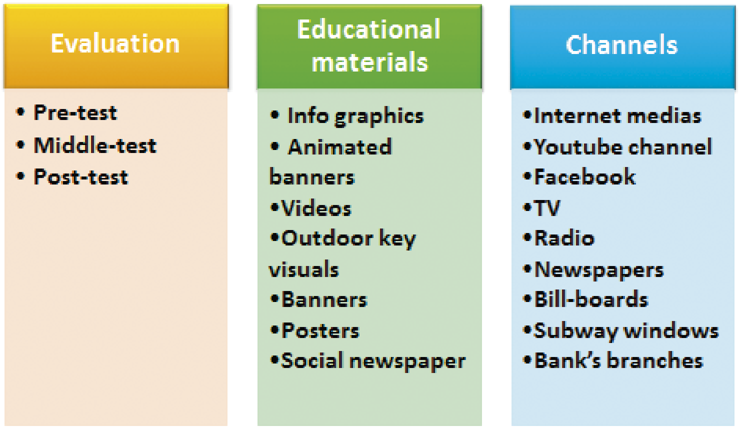
A preliminary analysis and forecast of the actual threats of payment instruments fraud was conducted, using information sources including the Ukrainian Interbank Exchange-online system, alerts and reports of EAST, Internet Organized Crime Threats Assessment (IOCTA) of EC3 Europol. We then analysed effective ways to measure awareness of citizens and to build a communication strategy with the aim of protecting citizens from payment fraud in Ukraine.

Based on the sociological study 'Fraud and Competence While Using Payment Instruments: A View of Ukrainian Consumers', conducted by GfK Ukraine for EMA, 2014, we understood that:

- Criminals exploit the ignorance of people about effective ways to recognise fraud in order to fraudulently obtain details of payment cards (the growth of fraud tripled in the first quarter of 2016 in comparison with the fourth quarter of 2015) or involve them unwittingly in criminal activities;
- Eleven per cent of cardholders are unaware of any means of protection against fraud; the remainder are aware of the existence of, on average, 1–2 per cent of protection means, while those protection means known to them are neither relevant nor effective against modern types of payment instruments and ATM fraud;
- Thirty-nine per cent of payment fraud victims will not seek help, and only 5 per cent of victims will report to law enforcement authorities.

During project implementation, project officer #2 responsible for this component of the project has achieved the following tasks:

- Three online researches (pre-test, middle-test, post-test) to measure the level of public awareness of the urgent and effective methods of recognising and



Evaluation
- Pre-test
- Middle-test
- Post-test

Educational materials
- Info graphics
- Animated banners
- Videos
- Outdoor key visuals
- Banners
- Posters
- Social newspaper

Channels
- Internet medias
- Youtube channel
- Facebook
- TV
- Radio
- Newspapers
- Bill-boards
- Subway windows
- Bank's branches

Figure 7: Project component #2: Citizens
Source: EMA

protecting against payment instruments and ATM fraud;
- Information campaign;
- Creation of awareness materials on the main fraud threats targeted cardholders: vishing, phishing websites, cash-trapping and skimming;
- Support of awareness campaigns of EC3 Europol: mobile malware, NoMoreRansom and European Money Mules Action for Ukrainian citizens.

The main messages that were used during the creation of awareness materials are shown in Table 1.

After conducting the information campaign in the first half of 2017, positive trends were identified (see Figures 8a and 8b).

Although a post-test of citizens' awareness is still being conducted to measure the final results of the awareness campaign, on the basis of middle-test we have seen that during #SafeCard, awareness of fraud signs and safe behaviour increased in places by more than 100 per cent, while awareness of the possibility of reporting payment fraud via the CyberPolice website increased by 40 per cent.

The third project objective was to improve the capacity of criminal justice professionals to obtain and check information when dealing with criminal proceedings related to ATM and payment instruments fraud (see Figure 9).

The research was based on analysis of a huge number of requests of the CPD concerning cash withdrawals completed by cards belonging to money mules or fraudsters, experience in coordination of joint investigations of LEAs and banks on skimming and usage of clone cards in the Ukrainian-acquiring network, results of the analysis of global software solutions for the rapid analysis of data on payment cards, and EMA's experience in preparation of expert reports concerning payment cards seized during arrests. The following points emerged:

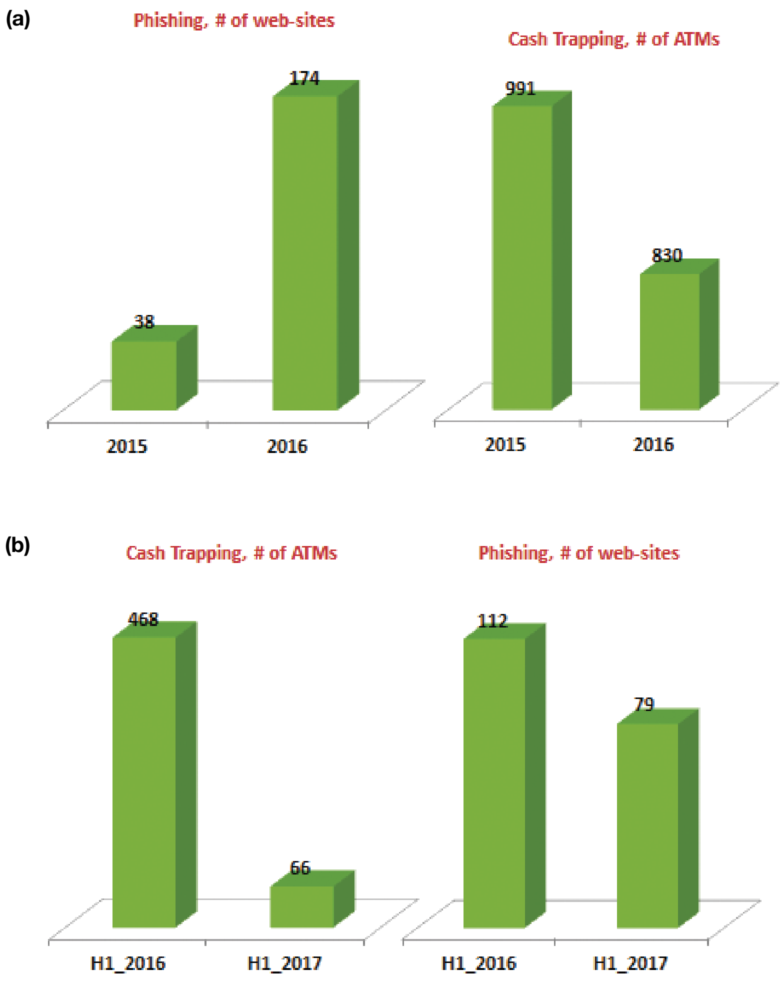
- Cyber police lack operational possibilities to identify a payment card issuer and send a request to determine place of cash withdrawals completed by cards belonging to money mules or fraudsters;
- LEAs have no technological possibility of rapidly verifying the content of the magnetic strip card data when detaining and searching persons near the ATM suspected of payment card fraud or money laundering resulting from cybercrime.

During project implementation, project officer #3 responsible for this component of the project has achieved the following tasks:

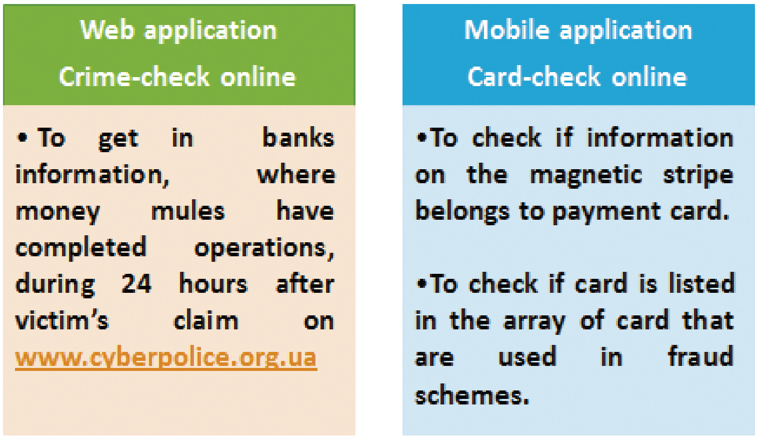
- Development of CrimeCheck-online — a web application for sending requests by the CPD of the National Police of Ukraine to banks in online mode concerning place of cash withdrawals by money mules or fraudster cards following a victim claim on the CPD website. CrimeCheck-online was implemented as a module of Interbank Exchange-online system, running on three major browsers (Internet Explorer, FireFox, Chrome);
- Development of CardCheck-online — a mobile application for quick examination

Table 1: Messages of awareness campaign

Vishing	✓ Card number is the only information you can share via phone. ✓ Never share expiry date, CVV/CVC2 and bank OTP from SMS with anybody — if somebody asks for this information via phone, stop the conversation immediately.
Phishing web-sites	✓ Check website before entering your card data.
Cash-trapping	✓ Never leave the ATM if your operation was successfully completed but you did not receive your money. Check dispenser and call the bank.
Skimming	✓ Protect your PIN by covering your hand with another hand or wallet.



Figures 8a and 8b: Fraud trends before and after #SafeCard
Source: EMA



Web application
Crime-check online

- To get in banks information, where money mules have completed operations, during 24 hours after victim's claim on www.cyberpolice.org.ua

Mobile application
Card-check online

- To check if information on the magnetic stripe belongs to payment card.
- To check if card is listed in the array of card that are used in fraud schemes.

Figure 9: Project component #3: Software
Source: EMA

and analysis by the patrol police staff, CPD and the Investigation Track1 and Track2 data on the magnetic strip of payment cards (see Figure 10).

The CrimeCheck-online module launched in July 2017 and during the first two months 1,154 requests from the CPD about cash withdrawals were successfully answered by 23 banks that had started to use the module in their everyday work. The maximum time frame for a response from the bank was 24 hours. Before CrimeCheck-online implementation, obtaining the same information normally took from few days to a few weeks.

During the pilot project of CardCheck-online, the application was installed and tested on 15 mobile devices running Android OS. Pilot usage is still being conducted by regional departments of the National Police of Ukraine. A version of the application for iOS is currently under development.

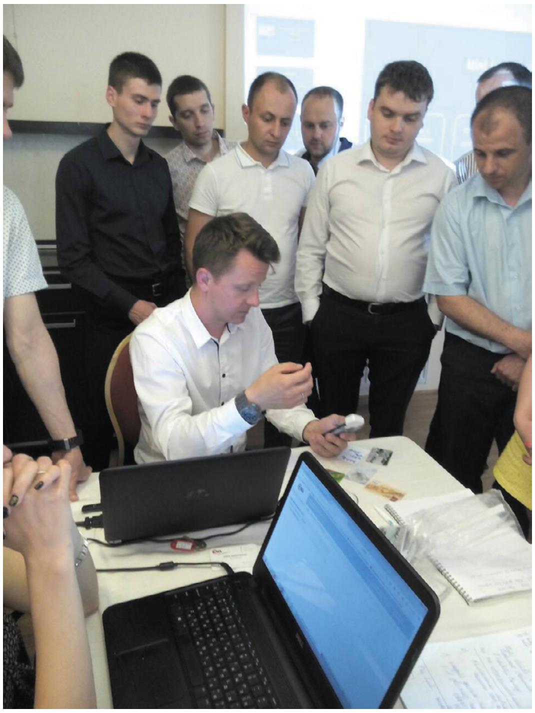


Figure 10: Project officer #3 gives instructions on how to use the CardCheck-online mobile application to representatives of LEAs during a regional workshop held in Lviv, June 20th, 2017. The workshop was conducted as part of the activities of component #4 of the project

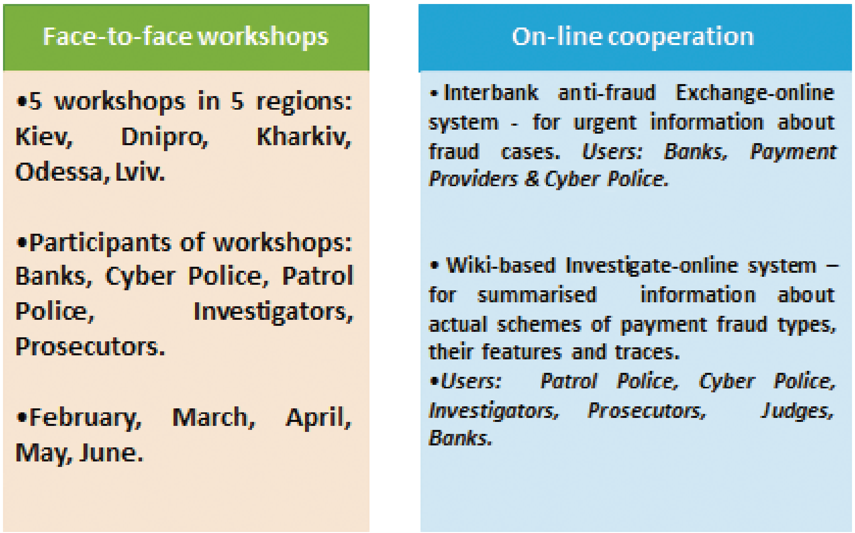
The fourth objective of the project was to improve the knowledge and skills of criminal justice professionals and their cooperation with banks dealing with criminal proceedings related to ATM and payment instruments fraud (see Figure 11).

EMA has 16 years' experience of coordinating interaction between the financial sector and LEAs in Ukraine for the detection and investigation of payment fraud cases, analysing actual threats of payment cards and ATM fraud in Ukraine (based on Interbank Exchange-online system information) and Europe (based on EAST and EC3 Europol alerts and reports), and sharing European classifications and best practices in investigation of payment fraud with banks and LEAs. Based on this experience, at the outset of the project the following observations were made:

- There are no developed operational cooperation mechanisms between LEAs and banks and payment aggregators to identify and investigate innovative types of crime related to payment cards and ATMs, such as vishing, smishing and phishing;
- Crime schemes related to payment cards and ATMs change and adapt to new payment technologies so quickly that traditional methods of knowledge sharing between banks and LEAs are no longer effective;
- LEAs need knowledge about signs and indicators of crimes related to payment cards and ATMs, which are recorded in the banking and processing systems, to provide more effective investigation of these crimes.

During project implementation, project officer #4 responsible for this component of the project has achieved the following tasks:

- Coordination of work of interdepartmental group comprising



Face-to-face workshops

•5 workshops in 5 regions: Kiev, Dnipro, Kharkiv, Odessa, Lviv.

•Participants of workshops: Banks, Cyber Police, Patrol Police, Investigators, Prosecutors.

•February, March, April, May, June.

On-line cooperation

• Interbank anti-fraud Exchange-online system - for urgent information about fraud cases. *Users: Banks, Payment Providers & Cyber Police.*

• Wiki-based Investigate-online system – for summarised information about actual schemes of payment fraud types, their features and traces.

•*Users: Patrol Police, Cyber Police, Investigators, Prosecutors, Judges, Banks.*

Figure 11: Project component #4: Cooperation between banks and LEAs
Source: EMA

EMA, patrol police and cyber police, with the aim of developing effective schemes for interaction between banks and LEAs to prevent and investigate payment and ATM crimes;

- Creation for LEAs of wiki-based online web application ‘Investigate-online’ and filling it with actual payment fraud scheme descriptions, signs and traces that are fixed in banking and processing systems;
- Conducting five workshops covering all regions of Ukraine in the five largest cities (Kyiv, Odessa, Kharkiv, Dnepropetrovsk and Lviv) with participation of the regional CPD, investigation departments, prosecutors’ offices, banks and EMA for knowledge sharing and the practical improvement of interaction mechanisms (see Figure 12). All workshops were followed by information campaigns across regional mass media: television, radio, Internet;
- Involvement of CPD regional employees in the interbank incidents exchange via ‘Exchange-online’ system and knowledge sharing via ‘Investigate-online’ (cyber-wiki);
- Creation of a draft document, regulating procedures of cooperation between companies within the financial sector and LEAs on questions of ATM and payment fraud.

Figure 12: Project officer #4 presents information about data compromise devices classification for representatives of LEAs during regional workshop in Kharkiv, 25th April, 2017.

As a result of this work, interaction understanding between banks and LEAs was improved, and time frames between the moment the crime was committed and the arrest of the criminals were reduced due to enhanced information exchange. The efficiency of crime investigation related to payment and ATM fraud increased, as well as the collection of appropriate evidence for further investigation by the courts.

The fifth objective of the project was to raise awareness of prosecutors and judges to problematic issues of qualification and criminal proceedings of ATMs and payment instruments crimes (see Figure 13).

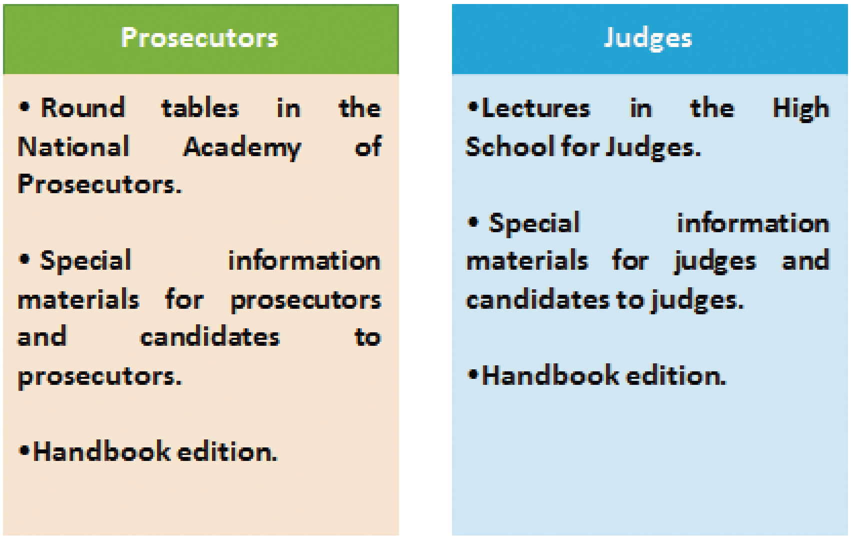
At this stage of the project preparation, statistical analysis of court decisions on payment and ATM fraud cases received from banking, LEAs and judicial systems, and comparative analysis of approaches to training and sentencing in countries with a Romano-Germanic legal system (the EU, CIS countries) were conducted. The form and volume of training provided on the topics of payment and ATM fraud by the National School of Judges of Ukraine and the National Academy of Prosecution of Ukraine were evaluated.

The following conclusions were drawn:

- Under certain crimes guilty persons are not punished at all, or punished disproportionately to the gravity of their acts;
- Identical or related offences are punished differently by different articles of the Criminal Code of Ukraine, proceeding from the general understanding of investigators, prosecutors and judges of legal relations in this field;
- General awareness about ATM and payment fraud schemes and traces in judicial and prosecutorial corps should be improved;
- Sources of specialised knowledge and reliable information about actual ATM and payment fraud schemes and their traces should be created.

During project implementation, project officer #5 responsible for this component of the project has achieved the following tasks:

- A questionnaire was prepared and 50+ judges of local and appellate courts were interviewed to determine the level of awareness of features and problematic aspects of the consideration of this category of criminal proceedings;
- Awareness materials in the form of presentations about actual payments and ATM fraud schemes for prosecutor and judge candidates were prepared;
- Three specialised lectures were conducted at the National School of Judges of Ukraine;



Prosecutors

• Round tables in the National Academy of Prosecutors.

• Special information materials for prosecutors and candidates to prosecutors.

•Handbook edition.

Judges

•Lectures in the High School for Judges.

• Special information materials for judges and candidates to judges.

•Handbook edition.

Figure 13: Project component 5: Prosecutors and judges
Source: EMA

- Four specialised workshops were conducted at the National Academy of Prosecution of Ukraine.

While completing these activities, it was clear that that level of awareness of prosecutors and judges regarding questions of payment technologies, actual payment and ATM fraud schemes, their features and traces was extremely low, although it rose significantly following the lectures and workshops (based on questionnaire results completed before and after). We understood that we had targeted just a small proportion of their representatives.

Our attempts to encourage them to work in the cyber-wiki 'Investigate-online' were not as successful as with the cyber police and investigators. We reached the conclusion that this category of professional person still requires a printed handbook, in the same way as they still use printed editions of Criminal Codes. We began work on the creation of a handbook for prosecutors and judges with an outline of the main principles of how international payment systems operate and crimes completed with the use of these payment instruments and infrastructure. We plan to complete and publish 250 copies of handbooks for prosecutors and 250 for judges in the near future.

CONCLUSION

Looking back and evaluating the results, we note that some tasks could be completed with less cost and more efficiency, especially in questions of public awareness. It is clear that work on raising awareness of prosecutors and judges has only just started, and to obtain the desired results we need to extend our efforts further and continue on a permanent basis, as we have with cyber police and investigation departments. But we also see how positive changes were implemented during 2017, so we will continue our work until we reach our vision of Ukraine tomorrow (see Figure 14).

Operations with payment instruments and ATMs in Ukraine are convenient and secure.

Figure 14: Ukraine tomorrow
Source: EMA