Ukrainian Interbank Payment Systems Member Association "EMA"

Ukrainian Banking

Payment Fraud Trends

Q1 2014

www.ema.com.ua

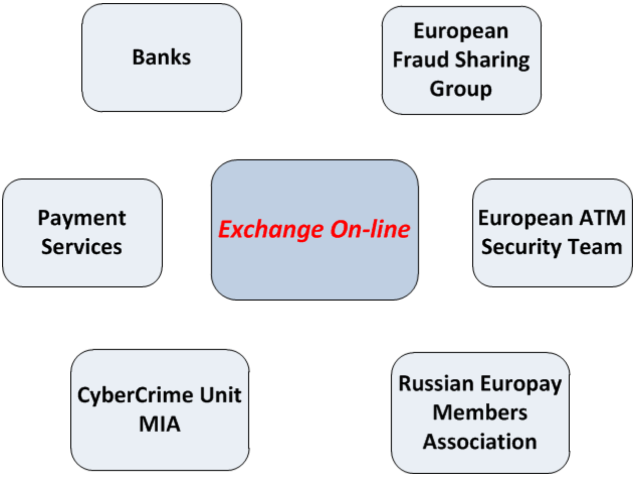
https://ibe.com.ua

www.ok2pay.com.ua

Data Source - Ukrainian Interbank Fraud Prevention System “Exchange-Online”

108 participants - banks, processors, payment services, MIA from

UA RU MD BY KZ


Banks

European Fraud Sharing Group

Payment Services

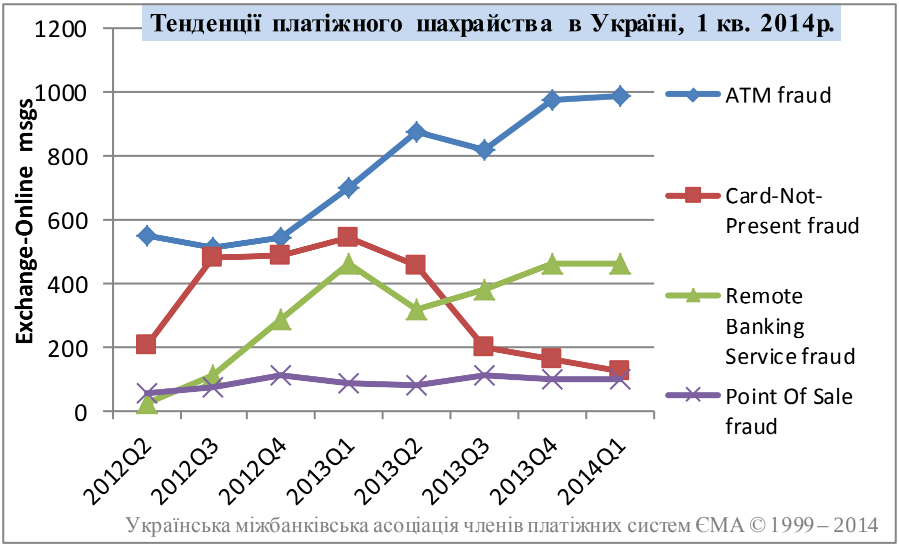
Exchange On-line

European ATM Security Team

CyberCrime Unit MIA

Russian Europay Members Association

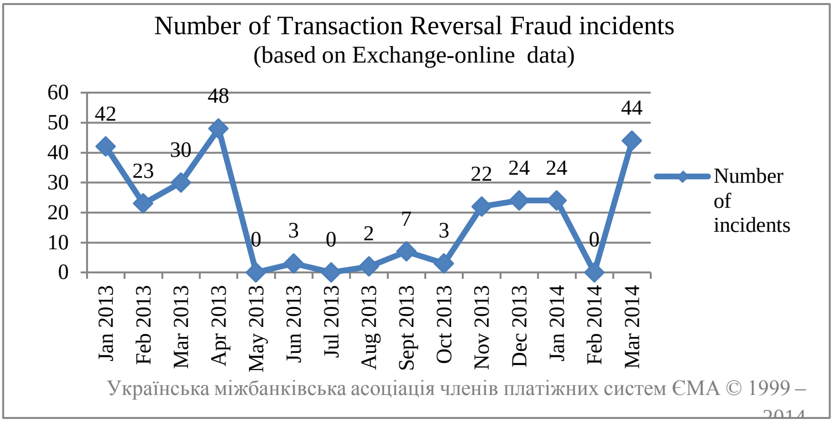
Payment Fraud Trends 2012-2014



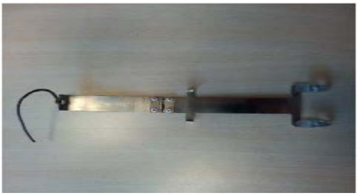
Українська міжбанківська асоціація членів платіжних систем ЄМА © 1999 – 2014

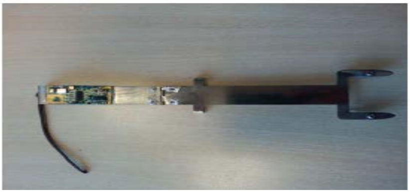
1. ATM FRAUD

1.1. Transaction Reversal Fraud (TRF)



In March 2014 in Russian Federation was picked up new modified device with microchip:





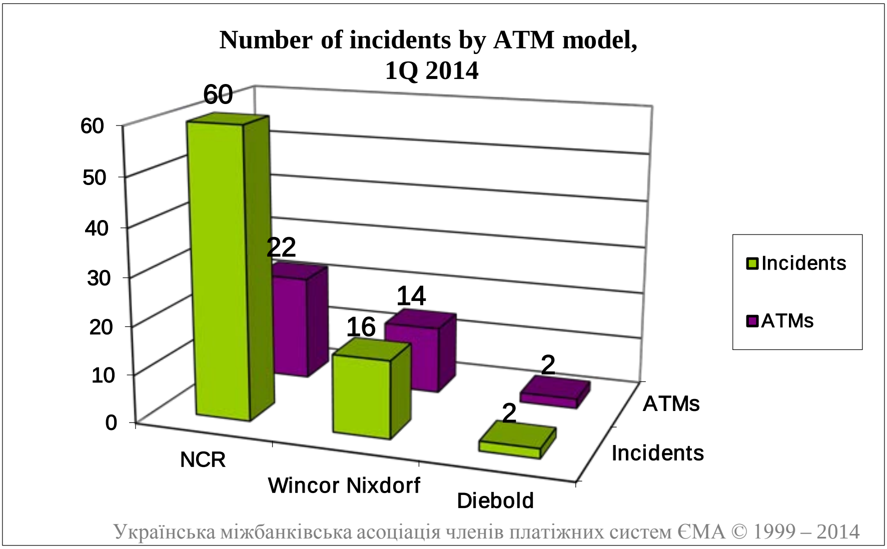
1.2. Cash Trapping

In Q1 2014 Ukrainian banks reported 10 cash-trapping incidents.

1.3. Skimming

1.3.1. Physical skimming

In Q1 2014 according to Exchange-online system data Ukrainian banks were faced with 78 skimming incidents on 38 ATMs.



1.3.2. Cyber skimming

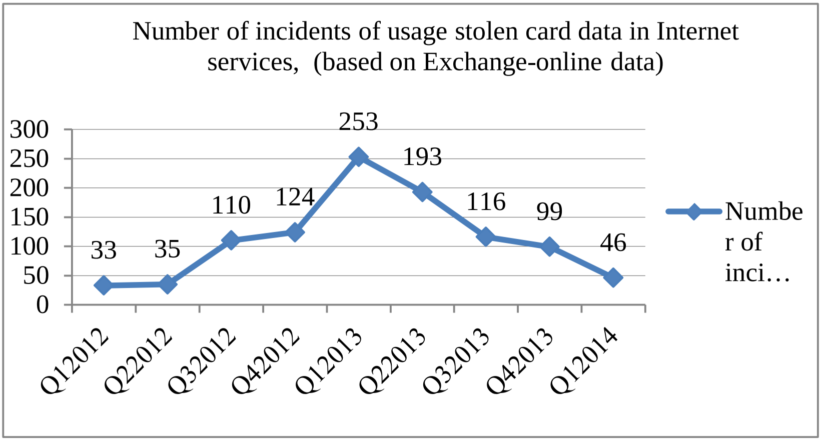
In February 2014 were detected cyber skimming facts on 29 ATMs Wincor Nixdorf. Malware used the same vulnerability of EPP keyboards as Trojan.Skimmer.18 for NCR ATMs.

Malware detection on Wincor Nixdorf ATMs was the result of common investigation of EMA Association banks on ATM data leaks in Kiev region during 2010-2013 years.

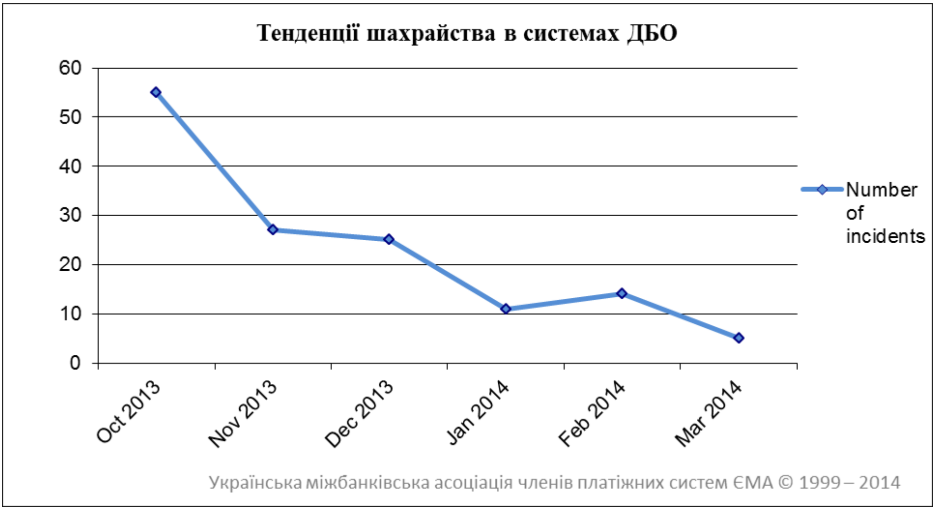
1.3.3. ATM direct dispense (Jackpotting)

Two banks were reported of two incidents of jackpotting. As the result more than 60 ATMs were emptied. Both incidents were possible by external intrusion into banking networks and taking further control of ATM networks.

2. CARD-NOT-PRESENT FRAUD



3. INTERNET-BANKING FRAUD



Internet-banking fraud trends, Q4 2013 – Q1 2014

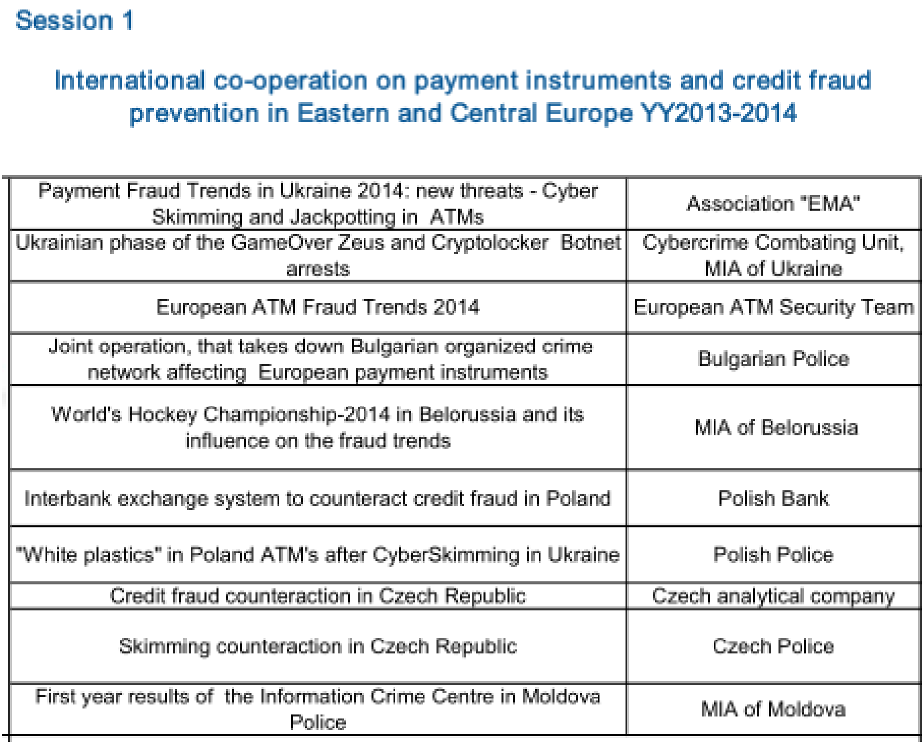
In 1Q 2014 there were registered eight DDoS attacks on banking services. All attacks had the aim to hide fraudulent internet-banking transfers.

VII EASTERN EUROPE EMA FRAUD CONFERENCE

18-19 September 2014 (Black Sea Bugaz, Odessa, Ukraine)

The Ukrainian Interbank Payment Systems Member Association "EMA" with the support of the Cybercrime Unit of the Ministry of Internal Affairs of Ukraine, the State Financial Monitoring Service of Ukraine, ICITAP (International Criminal Investigative Training Assistance Program) of Department of Justice of USA and EAST (European ATM Security Team) continues started previous years effective experience exchange between law enforcement agencies and private sector in the inter-country level**.**

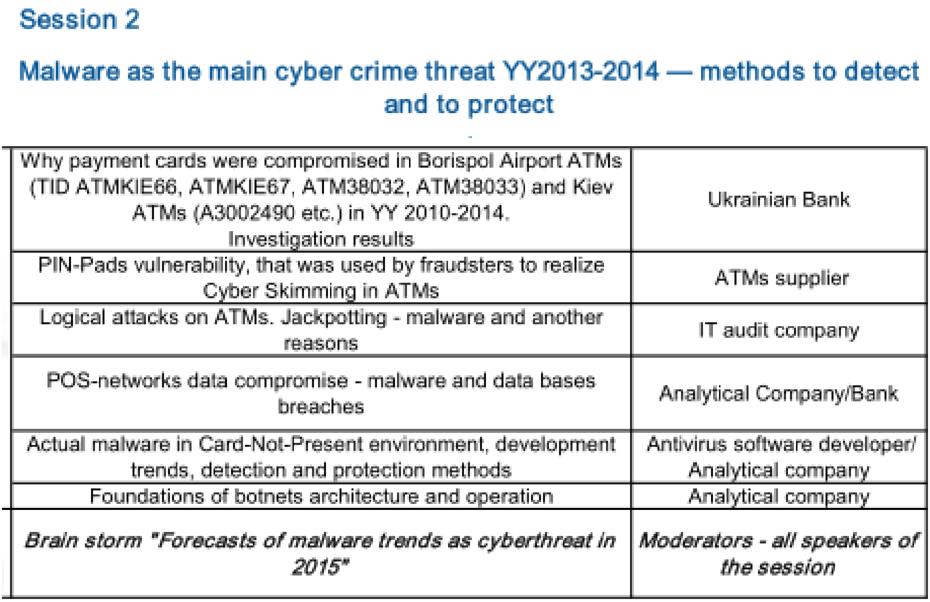
Day 1



Session 1

International co-operation on payment instruments and credit fraud prevention in Eastern and Central Europe YY2013-2014

Payment Fraud Trends in Ukraine 2014: new threats - Cyber Skimming and Jackpotting in ATMs	Association "EMA"
Ukrainian phase of the GameOver Zeus and Cryptolocker Botnet arrests	Cybercrime Combating Unit, MIA of Ukraine
European ATM Fraud Trends 2014	European ATM Security Team
Joint operation, that takes down Bulgarian organized crime network affecting European payment instruments	Bulgarian Police
World's Hockey Championship-2014 in Belorussia and its influence on the fraud trends	MIA of Belorussia
Interbank exchange system to counteract credit fraud in Poland	Polish Bank
"White plastics" in Poland ATM's after CyberSkimming in Ukraine	Polish Police
Credit fraud counteraction in Czech Republic	Czech analytical company
Skimming counteraction in Czech Republic	Czech Police
First year results of the Information Crime Centre in Moldova Police	MIA of Moldova

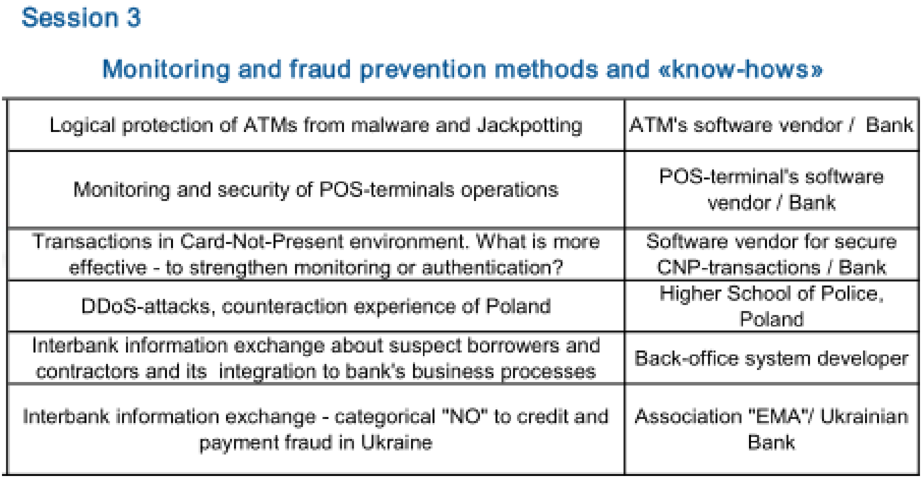


Session 2

Malware as the main cyber crime threat YY2013-2014 — methods to detect and to protect

Why payment cards were compromised in Borispol Airport ATMs (TID ATMKIE66, ATMKIE67, ATM38032, ATM38033) and Kiev ATMs (A3002490 etc.) in YY 2010-2014. Investigation results	Ukrainian Bank
PIN-Pads vulnerability, that was used by fraudsters to realize Cyber Skimming in ATMs	ATMs supplier
Logical attacks on ATMs. Jackpotting - malware and another reasons	IT audit company
POS-networks data compromise - malware and data bases breaches	Analytical Company/Bank
Actual malware in Card-Not-Present environment, development trends, detection and protection methods	Antivirus software developer/ Analytical company
Foundations of botnets architecture and operation	Analytical company
Brain storm "Forecasts of malware trends as cyberthreat in 2015"	***Moderators - all speakers of the session***

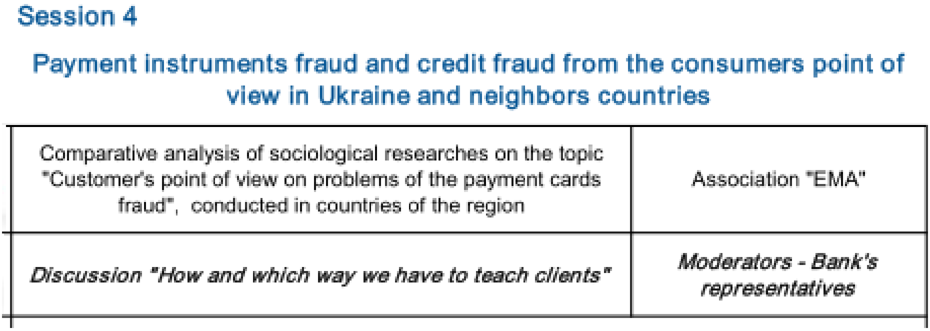
Day 2



Session 3

Monitoring and fraud prevention methods and «know-hows»

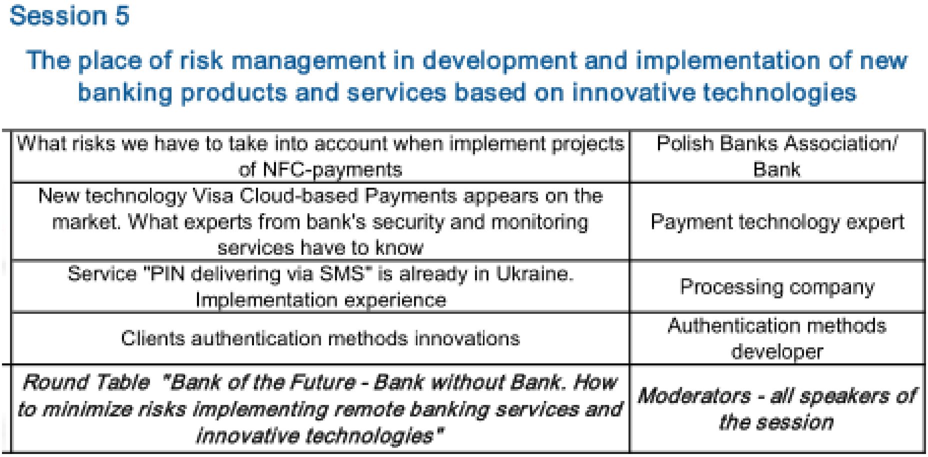
Logical protection of ATMs from malware and Jackpotting	ATM's software vendor / Bank
Monitoring and security of POS-terminals operations	POS-terminal's software vendor / Bank
Transactions in Card-Not-Present environment. What is more effective - to strengthen monitoring or authentication?	Software vendor for secure CNP-transactions / Bank
DDoS-attacks, counteraction experience of Poland	Higher School of Police, Poland
Interbank information exchange about suspect borrowers and contractors and its integration to bank's business processes	Back-office system developer
Interbank information exchange - categorical "NO" to credit and payment fraud in Ukraine	Association "EMA"/ Ukrainian Bank



Session 4

Payment instruments fraud and credit fraud from the consumers point of view in Ukraine and neighbors countries

Comparative analysis of sociological researches on the topic "Customer's point of view on problems of the payment cards fraud", conducted in countries of the region	Association "EMA"
Discussion "How and which way we have to teach clients"	*Moderators - Bank's representatives*



Session 5

The place of risk management in development and implementation of new banking products and services based on innovative technologies

What risks we have to take into account when implement projects of NFC-payments	Polish Banks Association/ Bank
New technology Visa Cloud-based Payments appears on the market. What experts from bank's security and monitoring services have to know	Payment technology expert
Service "PIN delivering via SMS" is already in Ukraine. Implementation experience	Processing company
Clients authentication methods innovations	Authentication methods developer
Round Table "Bank of the Future - Bank without Bank. How to minimize risks implementing remote banking services and innovative technologies"	*Moderators - all speakers of the session*

For more information please contact

Alexey Krasyuk
Information Security Advisor
+38044 568-58-38
okr@ema.com.ua