



iPROCEEDS

Project on targeting crime proceeds on the Internet
in South-eastern Europe and Turkey

Workshop on online financial fraud and credit card fraud

Provided under iPROCEEDS project
Sarajevo, 21-22 March 2018

Outline

Background and Justification

Cybercrime of today is driven mostly by financial gain and thus rapid detection and action on illegal money flows on the Internet often a necessity to identify and minimize damages from the criminal activity. Worldwide, most cybercrime reported and investigated by criminal justice authorities is related to different types of fraud and other offences aimed at obtaining illegal economic benefits. Online financial fraud and credit card fraud are highly profitable criminal activities and generating proceeds often being their primary purpose. In the past years the world saw an increase in CEO fraud, a crime which affects businesses of all sizes in both the private and public sector with tens of thousands of victims worldwide resulting in the loss of billions.¹ At the same time payment cards still remain a very popular payment method and therefore a target for criminals. Debit and credit cards skimming still represents a major threat. Card-present and card-not-present fraud is widely spread with forged cards and compromised credit card details being used to commit high volume crime, with tens of thousands of victims.

To respond effectively to these threats, co-operation is crucial between the law enforcement agencies and the industry through enhanced information sharing and public/private partnerships.

Expected Outcome

Carried out under Result 3 of the iPROCEEDS project *Cybercrime Units, financial investigators and financial intelligence units cooperate with each other at the domestic level in the search, seizure and confiscation of online crime proceeds*, the workshop is expected to:

- increase awareness of current threats, trends, countermeasures and various initiatives in the field of investigation and prosecution of online financial fraud and credit card fraud;

¹ FBI, Public Service Announcement, Business E-mail Compromise: The 3.1 Billion Dollar Scam, <https://www.ic3.gov/media/2016/160614.aspx>, 2016

- strengthen the capacity of the national criminal justice authorities to search, seize and confiscate online crime proceeds generated by such criminal activities;
- strengthen inter-agency cooperation among prosecutors, cybercrime unit, financial investigators and Financial Intelligence Department for the detection, prevention and fight against online financial fraud and its proceeds;
- improve information sharing between cybercrime related governmental agencies and the private sector entities at national level.

Participants

The event will be attended by the following participants:

- Cybercrime investigators;
- Prosecutors;
- Judges;
- Financial investigators;
- Financial intelligence specialists;
- Representatives of the banking sector.

Administrative arrangements and location

Hotel Novotel Bristol Sarajevo, Fra Filipa Lastrića 2, Sarajevo 71000, Bosnia and Herzegovina

Programme

Wednesday, 21 March 2018

09h00	Registration
09h30	Opening <ul style="list-style-type: none"> • Toni PAVLOSKI, Deputy Head of Office, Council of Europe Office, Sarajevo • Ramiz HUREMAGIC, Delegation of the European Union to Bosnia and Herzegovina
09h50	General overview of online financial fraud and credit card fraud in Bosnia and Herzegovina. Trends, statistics and case studies. <ul style="list-style-type: none"> • Representatives of the cybercrime units (Federation of Bosnia and Herzegovina, Republika Srpska, Brcko District) and Banking Association.
11h00	<i>Coffee break</i>
11h30	Social engineering, BEC/CEO fraud - a challenge for investigators. Public-private initiatives to detect and prevent CEO fraud. <ul style="list-style-type: none"> • Dawn JACKSON, Senior Officer, National Cyber Crime Unit Tactical Partnerships - Finance sector lead, National Crime Agency, UK • James WARREN, Senior Officer, Economic Crime Centre, National Crime Agency, UK.
12h30	<i>Lunch</i>
13h30	Online financial crimes and fraud - e-commerce fraud and online extortion. <ul style="list-style-type: none"> • Dawn JACKSON, Senior Officer, National Cyber Crime Unit Tactical Partnerships - Finance sector lead, National Crime Agency, UK • James WARREN, Senior Officer, Economic Crime Centre, National Crime Agency, UK.
14h40	Latest trends in credit card fraud - banking malware and skimming. <ul style="list-style-type: none"> • Gheorghe DESPA, Brigade for Countering Organised Criminality Ploiesti –

	Cybercrime Unit, Romania.
15h40	<i>Coffee break</i>
16h00	Online money laundering typologies. <ul style="list-style-type: none"> • Klaudijo STROLIGO, Council of Europe Expert
17h00	End of Day 1

Thursday, 22 March 2018

9h00	National legal framework for financial investigations of online crime proceeds. <ul style="list-style-type: none"> • Representatives of the Financial investigations Units
10h00	<i>Coffee break</i>
10h30	Investigations on the Darknet and criminal use of Bitcoins on the Darknet markets. Tracing methods to identify the suspect, technical seizure of Bitcoins. <ul style="list-style-type: none"> • Dominik HELBLE, State Criminal Police Office Baden-Württemberg Inspection 510, Cybercrime and digital traces, Cybercrime Investigations, Germany.
11h30	Financial investigations of online crime proceeds: tools, methods, challenges for law enforcement, inter-agency and international cooperation for the search, seizure and confiscation of online crime proceeds. <ul style="list-style-type: none"> • Roland BAIER, State Criminal Police Office Baden-Württemberg Inspection 740, Asset Forfeiture, Germany.
12h45	<i>Lunch and End of Day 2</i>

Contact:

Mariana CHICU
Project Manager
Cybercrime Programme Office
of the Council of Europe (C-PROC)
Email: mariana.chicu@coe.int
www.coe.int/cybercrime

Zlatka MITREVA
Senior Project Officer
Cybercrime Programme Office
of the Council of Europe (C-PROC)
Bucharest, Romania
Email: zlatka.mitreva@coe.int
www.coe.int/cybercrime