iPROCEEDS

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

www.coe.int/cybercrime

Version 15 May 2017

Activity 4.2.1

Assessment mission of guidelines to prevent and detect/identify online crime proceeds

22-23 May 2017, Sarajevo, Bosnia and Herzegovina

Provided under the iPROCEEDS project

Outline

Background

As the use of and reliance on information technology becomes ever more pervasive in society, the targeting and exploitation of computer systems has also become increasingly common. The Internet-based offences generate proceeds of crime and often the Internet is the place where the laundering process begins. Currently there is general agreement that generating proceeds is now the primary purpose of cybercrime.

Due to the rapid growth and technological developments, the payment systems developed tremendously in terms of speed of transactions, number and types of service providers, payment methods, clearing options and even currencies. These new developments of the payment systems offer opportunities for money launderers and render more difficult the detection of potentially suspicious transactions. In addition, cyber criminals combine within for the same schemes both traditional and new payment methods, co-mingling them in multiple operations including cash, bank transfers, prepaid cards, money remitters, e-currencies and other electronic payment systems. Therefore, the detection and pursuit of the criminal money flows is much more difficult for law enforcement agencies.

Financial sector institutions are bound to identify and report suspicious transactions to Financial Intelligence Units (FIUs) according to a set of indicators aimed at prevention of money laundering and terrorist financing. As regards cyber

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

laundering, red flags of anomalous behavior can be similar to the indicators in the traditional payment systems, or sometimes might bear some particular features. The quality and application of such indicators remains a challenge and it may be necessary to review indicators in order to better address specific risks related to new technologies and prevent and identify online crime proceeds.

Expected Outcome

Carried out under Result 4 – **Guidelines on the prevention and control of online fraud and criminal money flows for financial sector entities developed and disseminated, and indicators for the prevention of online money laundering reviewed and updated** - the assessment mission aims to gather specific information regarding the existing indicators and red flags for the financial sector institutions used to detect online fraud and money laundering in the online environment, as well as money laundering guidelines for obligators in Bosnia and Herzegovina with the view to review and update indicators for the prevention of online money laundering.

Participants

The consultants involved will meet various competent authorities and financial supervisors that are responsible to take regulatory and supervisory measures relevant to money laundering such as the Financial Intelligence Department (FID), Central Bank, regulators (e.g. gambling), licensing and supervisory agencies (capital market supervisors and the insurance sector supervisors), the private sector - Banking Association, as well as any other entity suggested by the host country.

Location

SIPA premises, Nikola Tesla Street No. 59, Sarajevo.

Programme

22 May 2017		
Time	**Participants**	**Topic**
09h30-10h30	Meeting with SIPA-Financial Intelligence Department	State of play in the area of Money Laundering, threats and online financial crimes and other cybercrime in the banking and financial sector.
10h30-11h30	Meeting with SIPA - Financial Intelligence Department, Federation Ministry of Interior, MUP Republika Srpska and Brcko District Police - experts in the field of cybercrime.	Cybercrime threats, trends and forms of online financial fraud in Bosnia and Herzegovina.
12h30-13h30	Meeting with SIPA - Financial Intelligence Department, Central Bank of Bosnia and Herzegovina, Banking Agency of the Federation of Bosnia and Herzegovina and Repulika Srpska.	State of play in the area of Money Laundering, threats and online financial crimes and other cybercrime in the banking and financial sector.
13h30-14h30	**Lunch**	

15h00-16h00	Meeting with SIPA - Financial Intelligence Department, Securities Commission of the Federation of Bosnia and Herzegovina; Commission for Securities of the Republika Srpska, the Commission for Securities of Brcko District.	State of play in the area of Money Laundering, threats and online financial crimes and other cybercrime in the capital markets sector.
16h15-17h15	Meeting with SIPA - Financial Intelligence Department, Bosnia and Herzegovina Insurance Agency, Insurance Supervision Agency in FBiH, Republika Srpska Insurance Agency, Association of Insurance Companies in Federation of Bosnia and Herzegovina, Association of Insurance Companies of Republika Srpska.	State of play in the area of Money Laundering, threats and online financial crimes and other cybercrime in the insurance sector.
23 May 2017		
Time	**Participants**	**Topic**
10h00-13h00	Representatives of the Council of Europe, SIPA - Financial Intelligence Department, the Banking Association of Bosnia and Herzegovina.	State of play in the area of Money Laundering, threats and online financial crimes and other cybercrime in the banking sector and the area of payment via the Internet.