iPROCEEDS

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

www.coe.int/cybercrime

Activity 4.2.1

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

19-20 June 2017, Pristina, Kosovo*[1]

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 laundering,

[1]*The designation is without prejudice to positions on status, and is in line with the ICJ Opinion on the Kosovo Declaration of Independence.

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

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 redflags 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 Kosovo* 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 Unit (FIU), Central Bank, regulators (e.g. gambling), licensing and supervisory agencies (capital market supervisors and the insurance sector supervisors), the private sector - Banking Association, money remittance providers, Internet payment services providers, as well as any other entity suggested by the national counterparts.

Programme

19 June 2017		
Time	**Agencies**	**Contact person and venue**
9h00-10h30	**Financial Intelligence Unit (FIU)** To discuss:money laundering guidelines for obligators,indicators of potential money laundering activity: money laundering red flags/ indicators	Str. Eduard Lir No. 1, Dragodan, Pristina
11h00-12h00	**Cybercrime Unit**, Kosovo* Police To discuss: cybercrime (online fraud) threats, trends and criminal money flows on the Internet in Kosovo*	Str. Eduard Lir No. 1, Dragodan, Pristina
12h30-13h30	**Central Bank** To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the banking and other financial sectors that are regulated and / or supervised by the Central Bank	Str. Eduard Lir No. 1, Dragodan, Pristina
13h30-14h30	**Lunch**	

15h00-16h00	**Insurance sector supervisors** To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the insurance sector that is regulated and / or supervised by the Insurance sector supervisor	Str. Eduard Lir No. 1, Dragodan, Pristina
20 June 2017		
Time	**Agencies**	**Contact person and venue**
9h00-10h00	**Banking Association** To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the banking sector	Str. Eduard Lir No. 1, Dragodan, Pristina
10h30-12h00	**Internet payment services providers** To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the Internet payment service sector	Str. Eduard Lir No. 1, Dragodan, Pristina