Activity 4.2.1

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

13 March 2017, Tirana, Albania

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, 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 Albania 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 Department of Prevention of Money Laundering of the Ministry of Finance, Central Bank, regulators (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 host country.

Programme

13 March 2017		
Time	**Agencies**	**Contact person and venue**
8h00-09h00	**Department of Prevention of Money Laundering – Financial Intelligence Unit** To discuss: money laundering guidelines for obligators, indicators of potential money laundering activity: money laundering red flags/ indicators	Deshmoret e Kombit Boulevard, No. 3 Ministry of Finance
09h15-10h00	**General Prosecution Office – Cybercrime Sector** To discuss: cybercrime threats, trends and criminal money flows on the Internet in Albania	Deshmoret e Kombit Boulevard, No. 3 Ministry of Finance
10h15-11h15	**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	Deshmoret e Kombit Boulevard, No. 3 Ministry of Finance
11h30-12h30	**Financial Supervision Authority** To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the financial sector that is regulated and / or supervised by the Authority	Deshmoret e Kombit Boulevard, No. 3 Ministry of Finance
12h30-13h30	**Lunch**	
13h45-14h30	**Chamber of Notaries** To discuss: money laundering threats, typologies and red flags related to online fraud and other	Deshmoret e Kombit Boulevard, No. 3 Ministry of Finance

	types of cybercrime in the notary sector that is regulated and / or supervised	
14h45-15h30	**Supervision Authority for Games of Chance** To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the gaming sector that is regulated and / or supervised by the gaming sector supervisor	Deshmoret e Kombit Boulevard, No. 3 Ministry of Finance
15h45-16h30	**Banking Association** To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the banking sector	Deshmoret e Kombit Boulevard, No. 3 Ministry of Finance
16h45-18h15	**Institutions of electronic payment (Easy Pay, M Pesa, M PAY, PAYLINK)** To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the electronic payment service sector **Money remittance providers** To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the remittances sector	Deshmoret e Kombit Boulevard, No. 3 Ministry of Finance