



iPROCEEDS

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

Activity 4.2.1

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

15-16 June 2017, Skopje

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

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

online environment, as well as money laundering guidelines for obligators “the former Yugoslav Republic of Macedonia” 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, Chamber of Commerce, money remittance providers, Internet payment services providers, as well as any other entity suggested by the national counterparts.

Draft Programme

15 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.	FIU
11h00-12h00	Cybercrime Sector To discuss: cybercrime (online fraud) threats, trends and criminal money flows on the Internet in “the former Yugoslav Republic of Macedonia”	Ministry of Interior
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	Central Bank
13h30-14h30	Lunch	
15h00-16h00	Capital market supervisor To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the securities market sector that is regulated and / or supervised by the capital market supervisor	Securities Exchange Commission
16h30-17h30	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	Insurance Supervision Agency

	supervised by the Insurance sector supervisor	
16 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	
10h30-11h45	Chamber of Commerce To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in designated non-financial organizations and professions (DNFBPs) sectors	
12h15-13h00	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	
13h00-14h00	Lunch	
14h30-15h15	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	Unija Finansiska Skopje
15h45-17h00	<i>Other entities</i> To discuss: money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in designated non-financial organizations and professions (DNFBPs) sectors	Le Grand Casino-Skopje