



iPROCEEDS

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

www.coe.int/cybercrime

Activity 4.3

Regional workshop on guidelines and indicators to prevent and detect online crime proceeds

**Provided under the iPROCEEDS project
in cooperation with the Office for Money Laundering Prevention
(OMLP) of the Republic of Slovenia**

4-5 October 2017

**GR – Ljubljana Exhibition and Convention Centre
Dunajska cesta 18, Ljubljana, Slovenia**

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.

Funded
by the European Union
and the Council of Europe



COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

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.

The Council of Europe carried out seven assessment visits in Albania, Bosnia and Herzegovina, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo*¹ and met various competent authorities and financial supervisors that are responsible to take regulatory and supervisory measures relevant to money laundering with the aim 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 with the view to review and update indicators for the prevention of online money laundering.

Expected Outcome

Carried out under Result 4 of the iPROCEEDS project – **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 objective of the regional workshop is to facilitate the review and update of indicators for the prevention of money laundering in the online environment.

In view of this, the objective of the workshop is to discuss the following aspects:

- Current cybercrime threats, trends and criminal money flows on the Internet in South-eastern Europe and Turkey;
- Money laundering threats, typologies and red flags related to online fraud and other types of cybercrime in the banking and other financial sectors in the region;
- Assessment of the existing guidelines, indicators and red flags for the financial sector institutions used to detect online fraud and money laundering in the online environment;
- Agree on the way forward with the view to update/develop indicators to effectively detect and prevent online fraud and money laundering on the Internet.

Participants

Financial Intelligence Units, cybercrime investigators and/or prosecutors, Central Banks, and the private sector - Banking Association from Albania, Bosnia and Herzegovina, Montenegro, Serbia, Slovenia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo*.

The working languages will be English and Slovenian. Interpretation into Albanian, Macedonian, Serbian and Turkish will be ensured.

¹ *This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

Programme

Wednesday, 4 October 2017	
9h00	Registration
9h30	Opening <ul style="list-style-type: none"> - Darko MUŽENIČ, Director of the Office for Money Laundering Prevention (OMLP) of the Republic of Slovenia; - Mariana CHICU, Project Manager, Cybercrime Programme Office (C-PROC) of the Council of Europe.
09h50	Session 1: General overview of cybercrime and money laundering threats, trends and typologies in the online environment and guidelines and indicators for the private sector to prevent and detect online fraud and criminal money flows on the Internet in the region. <ul style="list-style-type: none"> - Current cybercrime threats, trends and criminal money flows on the Internet in South-eastern Europe and Turkey; - Money laundering threats, typologies and red flags/indicators related to online fraud and other types of cybercrime in the banking and other financial sectors in the region. <p>Presentations by the Office for Money Laundering Prevention (OMLP) of the Republic of Slovenia and the project countries/areas (Central Banks, FIUs, cybercrime investigators/prosecutors, Banking Associations)</p> <p>Tour de table: Slovenia, Albania, Bosnia and Herzegovina and Montenegro (<u>15 minutes each</u>).</p> <p><i>Moderator: Klaudio STROLIGO, Council of Europe expert</i></p>
11h00	Coffee break
11h30	Session 2: Tour de Table of the delegations, cont'd <p>Presentations by project countries/areas Serbia, "The former Yugoslav Republic of Macedonia", Turkey and Kosovo* (Central Banks, FIUs, financial investigators and cybercrime units and Banking Associations) (<u>15 minutes each</u>) on:</p> <ul style="list-style-type: none"> - Current cybercrime threats, trends and criminal money flows on the Internet in South-eastern Europe and Turkey; - Money laundering threats, typologies and red flags/indicators related to online fraud and other types of cybercrime in the banking and other financial sectors in the region. <p><i>Moderator: Mariana CHICU, Council of Europe</i></p>
12h30	Lunch
14h00	Session 3: Common typologies for online financial fraud and other types of cybercrime in South-eastern Europe and Turkey. <p><i>Speaker: Hein DRIES, Council of Europe expert</i></p> <p>Presentations of findings following seven assessment visits by Council of Europe</p>

	experts. Discussions
15h00	Coffee break
15h30	<p>Session 4: Policy and organisational observations and challenges that impact the effective prevention and detection of online fraud and money laundering in the online environment in South-eastern Europe and Turkey.</p> <p><i>Speaker: Klaudio STROLIGO, Council of Europe expert</i></p> <p>Presentations of findings following seven assessment visits by Council of Europe experts.</p> <p>Discussions</p>
16h30	<p>Session 5: Assessment of the existing guidelines, indicators and red flags and recommendations for new indicators for the financial sector institutions to detect online fraud and money laundering in the online environment.</p> <p><i>Speaker: Klaudio STROLIGO, Council of Europe expert</i></p> <p>Presentations of findings following seven assessment visits by Council of Europe experts.</p> <p>Discussions</p>
17h15	Conclusions
17h30	End of day 1
19h00	Social dinner
Thursday, 5 October 2017	
9h30	<p>Session 6: Law Enforcement, Financial Intelligence Units and Financial Institutions working together to detect online fraud and money laundering in the online environment.</p> <p><i>Speaker: Klaudio STROLIGO, Council of Europe expert</i></p> <p>Discussions</p>
10h30	<p>Session 7: Public Outreach - Advisories to Citizens and Financial Institutions.</p> <p><i>Speaker: Hein DRIES, Council of Europe expert</i></p> <p>Discussion</p>
11h15	Coffee break
11h45	<p>Session 8: Measures and next steps for development/update of indicators to effectively detect and prevent online fraud and money laundering on the Internet.</p> <p>Working groups facilitated by Council of Europe experts.</p>

12h45	Lunch
14h00	Session 9: Measures and next steps, cont'd Reports from each working group. Session moderated by the Council of Europe experts
15h00	Conclusions
15h30	End of day 2
19h00	Social dinner in Bled

Contact

For any additional information please contact:

Mariana CHICU
Project Manager
Cybercrime Programme Office (C-PROC)
Tel: +40-21-201-7840
Email: mariana.chicu@coe.int

Zlatka MITREVA
Senior Project Officer
Cybercrime Programme Office (C-PROC)
Tel: +40- 21-201-7880
Email: zlatka.mitreva@coe.int