HOW TO COMBAT THE 'MONEY MULE' PHENOMENON

DR ATTILA SISÁK
Finance Guard Captain; Deputy Head of the Department for Criminal Affairs (Hungarian National Tax and Customs Administration, Directorate General of Criminal Affairs) Budapest

Keywords: *organized crime, 'money mules', money laundering, cybercrime, 'phishing', 'freezing order'*

TARGETED PROBLEM/ PHENOMENON

In recent years a relatively sophisticated type of criminality has been keeping the financial crime investigating service of the Hungarian National Tax and Customs Administration gradually occupied. An increasing number of internet scams appear to violate the trust invested in the transparent operation of financial service providers as well as exploiting the weaknesses of bank security mechanisms and the relatively slow reaction of national law enforcement agencies. The damage caused by these scams is escalating year after year.

Several commercial banks providing online banking services suffered 'phishing attacks' in the last couple of years. '*Phishers*' forge web pages used by customers for online banking and customers are deceived via these scam sites in order to provide their personal financial information (usernames, passwords etc.). Later, the customer's information is abused for unlawful and unauthorized transfers.

Frequently linked with the above mentioned fraudulent activity the '*money mule*' phenomenon is spreading rapidly, taking up various forms. For instance intermediary-agent jobs are advertised online. Money mules are mostly individuals who are recruited by fraudsters to help transferring fraudulently obtained money (most of the time online banking scams). After being recruited by the fraudsters (usually by using electronic means of communication), money mules typically receive funds into their accounts. Then they are asked to send it further to a third party; minus a certain commission payment. The '*straw men*' are usually honored with 5-10% intermediary commission for sending the amounts transferred to their bank accounts to Eastern and Northern European (typically Baltic, Russian, Ukrainian, etc) addresses via money transfer using money transfer services (e.g. Western Union, MoneyGram, etc.). They ensure that the money shall be provided to the addressees after personality verification (by means of passport) by a money transfer agent.

The diversified appearance of internet scams is inexhaustible, but this type of criminality has one thing in common. The fraudulently obtained money is usually 'chopped up' and sent to a countless number of previously hired money mules in order to blur the trail of money. Money eventually ends up in the hands of 'money collectors' (usually members of organised crime groups) who re-group the funds and invest (launder) them according to their needs.

LEGISLATIVE BACKGROUND/ RULES SETTING OUT THE CONDITIONS OF IMPLEMENTING THE SPECIFIC PRACTICE

It should be noted that domestic implementation of the international legislation listed below could differ in Member States in practice:

- Council Decision of 17 October 2000 (2000/642/JHA) concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information and Directive 2005/60/EC of European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (3rd AML Directive);
- Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union – implemented in Hungary;
- Council Framework Decision 2003/577/ JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence;
- Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to crime;
- Council Framework Decision 2003/577/ JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence;
- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. Warsaw, 16.V.2005.
- Criminal Code, other relevant domestic legislation that criminalizes money laundering and the internet fraud as an underlying predicate offence.

METHOD/ BEST PRACTICE DESCRIPTION

The only realistic chance to restrain such proceeds of crime in these cases is when the money is still in the banking sector, to be more precise when it is credited to the *'mule's'* account.

In most of these types of cases the victim residing in one MS tries to recall the money usually transferred to the bank account of the money mule in an another MS, and when it turns out that the money has already been credited to another account of a foreign beneficiary the originator bank sends a SWIFT message to the beneficiary bank and simultaneously the victim turns to the national law enforcement/investigating authority. If the money had not been withdrawn before the foreign bank sends its SWIFT-warning explaining that the transfer is a result of criminal activity, then the financial service provider can freeze the transaction, since in the event of noticing any information, fact or circumstance indicating money laundering the financial service provider has the authority to suspend the execution of a transaction order for a certain period of time as defined in the relevant country's national AML/CFT legislation. When the service provider considers the immediate action of the authority operating as the financial intelligence unit (FIU) to be necessary for checking the data, fact or circumstance indicating money laundering, it is required to file a Suspicious Transaction/Activity Report (STR/SAR) without delay to the FIU in order to investigate the cogency of the report. The bigger the time period of the suspension the better the chance in preventing. This timeframe could be extended when applying Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. Warsaw, 16.V.2005. *(Article 14 of the Convention regulating the postponement of domestic suspicious transactions states, that Each Party shall adopt such legislative and other measures as may be necessary to permit urgent action to be taken by the FIU or, as appropriate, by any other competent authorities or body, when there is a suspicion that a transaction is related to money laundering, to suspend or withhold consent to a transaction going ahead in order to analyze the transaction and confirm the suspicion. Each party may restrict such a measure to cases where a suspicious transaction report has been submitted. The maximum duration of any suspension or withholding of consent to*

a transaction shall be subject to any relevant provisions in national law.)

Within the above mentioned time period the FIU – by using its effective and fast communication channels (especially ESW, or the FIU.NET) – can very easily get in contact with the FIU of the victim's country and request information on the fraudulent activity (predicate offence), persons, bank accounts and the amount of money involved. It is even better if the starting bank provides extra information on whether the victim reported the crime to competent LEA (case No. and name of the investigating authority) or not.

In such cases there should be a mechanism in place which ensures that the FIU immediately discloses this information to the national Asset Recovery Offices (AROs) since it is an expectation that AROs should be able to cooperate effectively with Financial Intelligence Units and judicial authorities. AROs should exchange information rapidly, possibly within the time limits foreseen in Framework Decision 2006/960/JHA. This time limit, in line with the national time limit for suspending a suspicious transaction on the basis of the national AML/CFT requirements (in accordance with the 3rd AML/CFT directive, and Council decision 2000/642/JHA) should be kept in mind when taking the next step, which would be the application of Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence.

The least time consuming solution would be if – in accordance with national law – the ARO would take up the role of providing the essential data/information for the preparation of the freezing order and the Certificate (e.g. name and data of the authority competent for the enforcement of the freezing order, etc.) to the competent foreign judicial authorities via the ARO of the originator country since it knows its national system best. Of course a proactive FIU could also be a part of such procedure but based on Council Decision 2007/845 JHA (Article 1) AROs might be more easily accepted for this purpose. Besides AROs are expected to be invested with powers to provisionally freeze assets on their own (e.g. for at least 72 hours) in order to prevent dissipation of the proceeds of crime between the moment when assets are identified and the execution of a freezing or confiscation court order. They should also be able to conduct joint investigations with other authorities. These characteristics – which basically are characteristics of law enforcement authorities (LEAs) - make AROs more effective mediators in such cases to obtain the necessary documents from the judicial authorities in order to secure the assets for the duration of the criminal investigation.

CRUCIAL SUCCESS FACTORS/ CONCLUSION

It is vital that the whole process should be carried out within the time frame of the suspension of the suspicious transaction which differs from country to country, therefore it is essential that the competent authorities are aware of the relevant national provisions existing in different MSs setting out the rules for suspending unusual/suspicious transactions that may relate to ML or TF (presumably regulated in the domestic AML/CFT legislations).

Raising awareness among financial service providers, FIUs, AROs, LEAs and judicial authorities is inevitable. Since these types of criminal actions constitute ML in the country where the transaction arrives and on the grounds of the 40 FATF Recommendations they are integrant part of the AML/CFT mechanism, therefore must be included in the ML typologies.

The above detailed formalized procedure could be a very well working mechanism when dealing with fraudulent criminality using internet (internet fraud).