

## **Electronic Funds Transfer in Money Laundering Crime: Regulation Needed in Response to Meeting of Technology and Crime in Indonesia**

Go Lisanawati  
University of Surabaya  
E-Mail: go\_lisanawati@ubaya.ac.id

### **ABSTRACT**

Advancements in information technology have affected modern society in numerous areas, including communication, education, commerce, and so on. These advancements have brought incredible benefits; they have also provided opportunities and motivation for various forms of crime. Information technology has also made crime highly profitable. Among the many types of criminal activities, modern technology has allowed money laundering to become an online crime. This new type of crime has raised some legal questions about the capability of national and international regulations in relation to current and upcoming issues. These include finding electronic funds transfer records after the fact, and determining money laundering activity that includes electronic funds transfer. Although Indonesia is an integral member of a community concerned with the interaction between technology and money laundering, it has not provided regulations to deal with the current and upcoming issues involving the crime of electronic money laundering. The increase in the amount of crime indicates the following series of techniques and mechanisms that had been detected in relation to money laundering activity. This research will examine current issues under the light of Indonesian regulations, and will put forward some proposals to close the legal vacuum.

**Keywords:** Electronic Funds Transfer, Money Laundering, Technology and Crime Interaction, Regulation Needed

## INTRODUCTION

In this era of globalization, the rapid dissemination of information is necessary. This could be carried out by using sophisticated technology such as the Internet. Prentice Hall's Illustrated Dictionary of Computing (Nader, 1995) states that the "Internet is the world's largest interconnected computer environment. It consists of millions of computers and tens of millions of users." By means of the Internet, people in every hemisphere are connected virtually. Naturally, such technology is useful for humans. Sanusi (2007) explains that: "The development of information technology has brought huge changes in society and has broad implications economically, socially, and legally." Information technology in the context of globalization is supposed to be a nice partner for humans. Technology is manifested as an important part of various human activities, i.e., electronic transactions. In fact, on the basis of efficiency and effectiveness, it could be claimed that electronic transactions will replace almost all business transaction activities.

The increases in technology have also created electronic forms of money. Electronic and other non-face-to-face financial services are included in electronic banking services, which can be used to facilitate money laundering. It is often difficult to identify the money laundering modus, because sophisticated technology is used to conceal the origin of the money. In the banking world, electronic money has become a cyberpayment instrument. Concerning such cyberpayments, Molander et al. (1999) in their RAND Monograph Report explained:

*Cyberpayments are an emerging new class of instruments and payment systems that support the electronic transfer of value... Because of the efficiency and ease with which they transfer value, Cyberpayment systems also present new challenges to law enforcement. Technology exists which could permit these systems to combine the speed of the present bank-based wire transfer systems with the anonymity of currency. As a result, there are issues that must be addressed as these systems are being developed to ensure the prevention and detection of money laundering and other illegal financial transactions.*

Banking systems have also changed fundamentally, with almost the entire process of implementing a payment system now carried out online. The challenges facing globalization and information technology, or the Internet, are so great that they defy the capacity of law enforcement alone to control. This is also true of regulation. The research question that should probably be discussed here is: **"How importance is the regulation**

**of electronic funds transfer in Indonesia in order to prevent money laundering?”**

## **THE MEETING OF MONEY LAUNDERING CRIME AND TECHNOLOGY AS A REVOLUTION OF MODERN CRIME**

The growth of technology in the world in conjunction with scientific growth has had an influence on human beings, especially in relation to changes in attitudes and the giving of meaning to technology. People consider technology to be a goal, rather than a tool. The technological change, especially in the field of information technology, has not yet been balanced by legal instruments.

The negative impact of rapid technological development is seen in changes in human behaviour, which tend to be criminal, and especially in the context of money laundering crime. In accordance with its characteristic, money laundering occurs as a modern, complicated, complex, and borderless crime. The complexity of modern crime that was produced by increases in technology has produced the consequence that put the positive law behind the society development. This has caused a legal vacuum. There is no regulation, yet cases are frequent and on the increase.

In relation to the Internet in the context of money laundering crime, Sressens (2000) explains:

*... This is not possible anymore with regard to the enormous gain from organised crime. Without sophisticated money laundering operations, which give these gains an apparently legitimate origin, the amount of profits of organised crime would in itself be an indication of their illegal origin...*

*Given the intrinsic link between organised crime and money laundering, the incrimination of money laundering itself should be considered as a new tool or even a new strategy in the fight against organised crime...*

Concerning the money laundering issue, Kader Asmal, as quoted from the book *Anti Money Laundering: International Law and Practice*, (2007) explains as below:

*... Criminals must therefore have access to financial resources in order to survive and grow. In this way the scourge of money laundering works to perpetuate all manner of criminal activities of the most serious nature ... The consequences of money laundering include greater risks to the soundness of financial institutions and contamination of legal finance transactions, while*

*legitimate business gets displaced to more secure jurisdiction.*

In combating money laundering, it is important for law enforcement agents to use the principle of “Follow the Money.” This principle is related to the mindset that money laundering has assumed the characteristic of the artery of crime or the blood of crime itself. In point of fact, there is no universal definition of money laundering. Various definitions for money laundering can be found in money laundering regulations, the opinions of legal scholars, and literature dealing with money laundering. Bucy (1998) defines money laundering as follows: “Money laundering is the concealment of the existence, nature, or illegal source of illicit funds in such a manner that the funds will appear legitimate if discovered.”

Money laundering involves various well-established and complex stages. The Asian Development Bank (2003) explains that “money laundering is a dynamic three-stage process that requires: Placement, moving the funds from direct association with the crime; layering, disguising the trail to foil pursuit; and integration, making the money available to the criminal once again with its occupational and geographic origins hidden from view.” In other words, the illicit funds re-enter the legitimate economy.

### **ELECTRONIC FUNDS TRANSFER CRIME IN MONEY LAUNDERING**

The Financial Action Task Force (FATF) on Money Laundering, in its recommendation no. 8, specifically focused on the possibility of the emergence of an upper exploitation cyber payment system for money laundering. Their recommendation is as follows:

*A Financial Institution should pay special attention to any money laundering threats that may arise from new or developing technologies that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, a financial institution should have policies and procedures in place to address any specific risk associated with non face to face business relationships or transactions.*

That recommendation warns about the sophisticated and anonymous crimes that might appear from developing technology. The Fraud Advisory Panel (2007), in its report, explains the impact of cybercrime in money laundering schemes as below:

*Computer enabled fraud comes in many forms. Examples of such frauds range from get-rich-quick schemes that don't exist to emails that demand an additional fee to be paid by credit card or personal details including passwords and account numbers... As mentioned above, money laundering is also covered by the act. This means that any organization whose services can be utilized by criminals to launder money will need to be aware of the legislation.*

From the explanation above, it is clear that there is a relationship between technology and money laundering. The Financial Action Task Force (FATF), in its Annex concerning issues of typology concerning payment technology, explained that there is the possibility of the emergence of a potentially powerful and new technique in money laundering known as a cyberpayment system. This could potentially aid criminals to hide the proceeds of their crime and move funds without detection.

Triyono (2008) then mentions: "The cyberpayment system is a new phenomenon. It does not require a regulated third party presence to transfer financial value among parties. It is also a potentially emerging money laundering technique." The proliferation of electronic funds transfer systems will enhance the risk that such transactions may be intercepted and diverted. On the other hand, emerging technologies could also greatly assist in concealing the origin of money laundering. Grabosky (1999) explained: "For some time now, electronic funds transfers have assisted in concealing and in moving the proceeds of crime. Emerging technologies will greatly assist in concealing the origin of ill-gotten gains. Large financial institutions will no longer be the only ones with the ability to achieve electronic funds transfers transiting numerous jurisdictions at the speed of light."

In the second stages of money laundering, it can be seen that the transfer of money is the heart of money laundering. Unfortunately, the regulation of electronic funds transfer is just in the form of the Bank of Indonesia Regulation (or the Peraturan Bank Indonesia – PBI), not in the form of an Act. Mutatis mutandis is not sufficient to prevent the crimes that have occurred. The Bank of Indonesia regulation has not prevented crime, and it has not provided sanction enough when enforced.

## **REGULATION OF ELECTRONIC FUNDS TRANSFER NEEDED AS A TOOL TO PREVENT MONEY LAUNDERING**

Article 1 sub paragraph 6 of Law Number 23 of the 1999 juncto Law Number 3 of 2004 concerning the Bank of Indonesia explains that: “The payment system is a system that includes a set of regulations, the agency, and the mechanism that is used to implement funds transfer in order to carry out an obligation that emerged from an economic activity.” Article 7 and Article 8 of the Bank of Indonesia Act explains that the Bank of Indonesia has the task to arrange and supervise the payment system to reach and maintain the Stability of the Rupiah.

In fact, funds transfer activities in Indonesia have been taking place over a long time period and with great frequency. The issue of electronic funds transfer regulation has been a major issue in this sense. There is a large amount of funds transfer activity but no regulation yet. This legal vacuum could potentially create crime.

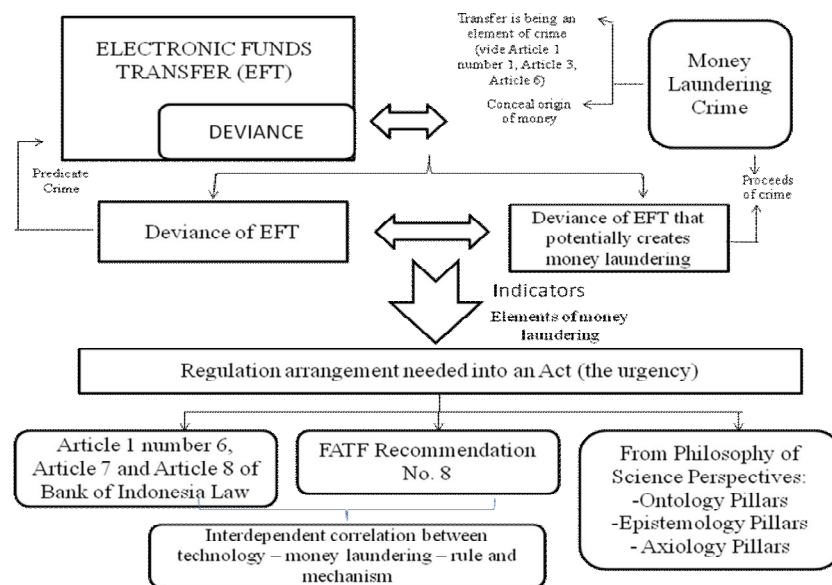
From the Philosophy perspective, the urgency of regulating electronic funds transfer into a legal norm could be viewed from the aspect of protection. This is related to facilities that utilize information technology and communication for electronic funds transfer. These facilities are easy, cheap, and fast. The problem of electronic funds transfer is very complex and has the potential to produce risks as well as the benefits that come from such rapid technology.

In line with the urgency of electronic funds transfer regulation, from the Philosophy of Science view, it could be understood that an Act to regulate electronic funds transfer is needed and could be used as a tool to anticipate money laundering crime. From Ontology pillars, the activity of transfer is mentioned as element of money laundering in Indonesian Money Laundering Law. Therefore, the transfer element is significant and could be used as the proof of criminal money laundering. From the Epistemology pillars, transfer activity is mentioned as one of the stages in money laundering crime. In the general explanation of the Republic of Indonesia Law Number 15 of the 2002 juncto Law Number 25 of 2003 concerning Money Laundering, the stage of layering is called the transfer stage. In the Money Laundering Law, the layering stage was identified as one of the most difficult phases to trace and prove. On the other hand, the Money Laundering Law did not provide a definition of a transfer. From the Axiology pillars, the existence of electronic funds transfer regulation, dealing with the activity of funds transfer along with the deviations prohibition, is essentially expected to prevent electronic funds transfer itself and also money laundering crime.

From the explanation above, Indonesia needs to regulate the activity of electronic funds transfer into an Act or Law, not only in an Internal Regulation such as the Bank of Indonesia Regulation, which regulates the Bank of Indonesia - Real Time Gross Settlement (BI- RTGS), National System of Clearance, and other payment products. This internal regulation could not be categorized as a criminal law regulation.

Indonesia already has the Electronic Information and Transaction Act Number 11 Year 2008 but this is not able to prevent electronic funds transfer crime. The underlying transaction may cause an upper transaction called an electronic funds transfer. As identified by its characteristic, an electronic funds transfer is not the same as an electronic information transaction. Electronic funds transfer requires its own regulation. The characteristics of electronic funds transfer are complex, involving numerous parties and the potential for abuse.

The explanations and reasons that regulation is needed can be understood by this diagram:



**Figure 1 Reasons that regulation is needed for EFT in Indonesia.**

## CONCLUSION

The commission of money laundering crimes has produced concern in societies around the world. The nature of money laundering, which has been manifested in the form of serious and complex crime, is becoming easier because of advances in

technology. Sometimes it might be manifested in the payment instruments in a financial system, which is money laundering, and could also be mixed with electronic funds transfer. The activity and possibility of electronic funds transfer deviance should be regulated. Consequently, to meet these aims, the Indonesian government should give attention to money laundering issues as they relate to sophisticated technology, such as electronic funds transfer crime modus. The Indonesian government should immediately regulate electronic fund transfer crime using a single Act.

### REFERENCES

- Asian Development Bank (2003). *Manual on Countering Money Laundering and the Financing of Terrorism*. Retrieved May 29, 2008, from <http://www.odccp.org>
- Bucy, P. H. (1998). *White Collar Crime: Case and Materials, 2<sup>nd</sup> Edition*, St. Paul Minn: West Publishing Co.
- Grabosky, P. (1999). *Crime in Cyberspace: Some Thoughts About Crime Prevention in Cyberspace*. Retrieved April 23, 2009, from <http://www.abc.net.au>
- Molander, Roger C., Mussington, B. David, & Wilson, Peter A. (1999). *Cyberpayment and Money Laundering: Problems and Promise, RAND Monograph Reports*. Retrieved January 12, 2007, from <http://www.rand.org>
- Muller, W. H., Kalin, C. H., & Goldsworth, J. G. (2007). *Anti Money Laundering: International Law and Practice*. Library of Congress Cataloging in Publication Data: England.
- Nader, J. C. (1995). *Prentice Hall's Illustrated Dictionary of Computing, 2<sup>nd</sup> edition*. National Library of Australia: Australia.
- Sanusi, M. A. (2007). *Konvergensi hukum dan Teknologi Informasi (Sebuah Torehan Empiris-Yuridis)*. The Indonesian Research: Jakarta.
- Stessens, G. (2000). *Money Laundering: A New International Law Enforcement Model*. Cambridge University Press: United Kingdom.
- The Fraud Advisory Panel (2002). *Cybercrime and The Proceeds of Crime Act: A Practical Guide for Business*. Retrieved April 7, 2007, from <http://www.fraudadvisorypanel.org>
- Triyono, A. (2008). Money Laundering dan Kemajuan Teknologi Informasi. *Jurnal Komunitas Anti Pencucian Uang*, 1(1), 115.