TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 37, 2022

A new decade for social changes

ISSN 2668-7798

www.techniumscience.com

Technium Social Sciences Journal
Vol. 37, 287-299, November, 2022
ISSN: 2668-7798
www.techniumscience.com

Bank role in preventing money laundering and cyber security

Muhammad Akbar Ilma, Murtanto, Titik Aryati

Trisakti University, Indonesia

akbarilma@yahoo.com, murayo2003@yahoo.com, titik.aryati@trisakti.ac.id

Abstract. The purpose of this study is to examine the effect of AML disclosure and cyber security on bank performance and to test whether intellectual capital strengthens or weakens the effect of AML disclosure and cyber security on bank performance. This study uses a sample of banking companies listed on the Indonesia Stock Exchange (IDX). The sample used is 41 banking companies listed on the Indonesian stock exchange. The findings of this study are (1) there is an effect of AML disclosure on Bank Performance. (2) there is no influence of cyber security on bank performance. The limitations of this research do not cover all types of banking in Indonesia, there are still many banking companies in Indonesia but they are not listed. The regulatory implications related to money laundering are the implementation of anti-money laundering programs in the financial services sector could be extended become a disclosure.

Keywords. anti-money laundering, bank performance, risk based bank rating

1. Introduction

In the current era of globalization, financial transactions are very easy to do, only in the grip of a cellular phone, individuals can do book-entry between one bank to another. Banking is the backbone of a nation's economy, banking has the task of collecting funds from the public and channeling funds to people who need these funds. Along with the current development of the banking industry, there are many banks in Indonesia, ranging from state-owned banks, foreign banks, private banks, and people's credit banks. All of them are vying for funds from the community and competing to get the flow.

In the industrial revolution 4.0, banks do not only compete with banks, but the emergence of financial technology or commonly called fintech is also a rival to banks that have already been established. The fintech is not only in the business of distributing funds to the public, but also as a payment channel or commonly referred to as a payment gateway so that it is as if fintech is a digital-based bank. With the increasingly rapid development of technology, banks also carry out many transformations so that they become sophisticated entities that have platforms that make it easier for their customers to conduct financial transactions.

With the ease of conducting financial transactions with banks, it does not mean that it only has a positive impact such as an increase in fee base income from banks, but there is also a negative impact, one of which is security in financial transactions. Not only customers who are harmed by the impact of ease of transaction such as fraud, but banks also have a significant risk of

Technium Social Sciences Journal
Vol. 37, 287-299, November, 2022
ISSN: 2668-7798
www.techniumscience.com

impact because they do things that are not in accordance with applicable regulations. As from cases of crime in banking, namely the crime of money laundering from the proceeds of illegal activities.

The Indonesian government has a significant role in protecting banks and their customers from illegal acts, especially money laundering as outlined in Law no. 8 of 2010 concerning the prevention and eradication of money laundering. This is intended to prevent the occurrence of actions that meet the elements of a criminal act for obtaining money from illegal or illegal ways. This must be prevented because the crime of money laundering originating from illegal transactions such as corruption and buying and selling narcotics needs to be narrowed down in order to minimize the flow of funds originating from activities that meet the criteria for criminal acts.

The Financial Services Authority or OJK also clarifies the practices that must be practiced by banks as stated in POJK No. 12/POJK.01/2017 concerning the implementation of anti-money laundering and prevention of terrorism financing programs in the financial services sector. With the complexity of the products offered by banks, it is possible that there will be loopholes to commit fraudulent acts, one of which is money laundering. Risks arising from the products offered by banks must be balanced with good risk management, such as monitoring transactions carried out by PPATK or commonly referred to as a financial transaction and analysis reporting center.

The Indonesian government has a significant role in protecting banks and their customers from illegal acts, especially money laundering as outlined in Law no. 8 of 2010 concerning the prevention and eradication of money laundering. This is intended to prevent the occurrence of actions that meet the elements of a criminal act for obtaining money from illegal or illegal ways. This must be prevented because the crime of money laundering originating from illegal transactions such as corruption and buying and selling narcotics needs to be narrowed down in order to minimize the flow of funds originating from activities that meet the criteria for criminal acts.

Money laundering is the act of disguising or obscuring, or hiding money or assets originating from a criminal act. In the crime of money laundering, it is carried out through three processes, the first is placement, which is an effort to place cash originating from a crime into the financial system (financial system), or an effort to place demand deposits (cheques, bank drafts, certificates of deposit). , etc.) back into the financial system, especially the banking system. Second, layering (transfer) is an effort to transfer assets originating from criminal acts (dirty money) that have been successfully placed with Financial Service Providers (especially banks) as a result of placement efforts to other Financial Service Providers. An example is to make several transactions or transfer funds. Third, integration is an effort to use assets originating from criminal acts that have managed to enter the financial system through placement or transfer so that they appear to be clean money, for lawful business activities or to refinance. criminal activity. An example is by purchasing assets and opening/conducting business activities (A. Rahman, 2014; Abu Olaim & Rahman, 2016; Bidabad, 2017; Samantha Maitland Irwin et al., 2011; Simwayi & Wang, 2012; Teichmann, 2017; Williams , 2009; Young, 2013; Zolkaflil et al., 2019).

One form of support or a way to prevent money laundering is to make rules based on the rules that apply at home and abroad in a transparent manner (Nobanee and Ellili, 2018). AML disclosure is one of the tools to reveal the role of banks in preventing money laundering. The disclosure is intended not only for regulators but for all stakeholders of the banking sector itself. Starting from shareholders, company management, employees, customers, and the community. AML disclosure is prepared based on the mutual agreement contained in the FATF recommendations (Financial Action Task Force). In international relations there are disclosures

TECHNIUM SOCIAL SCIENCES JOURNAL
Technium Social Sciences Journal
Vol. 37, 287-299, November, 2022
ISSN: 2668-7798
www.techniumscience.com

regarding money laundering designed by the Basel Institute. The disclosures designed by Basel have a fairly large level, namely at the level of a country.

The research gap in previous studies has reviewed many regulations related to the crime of money laundering, then there is still little research that has been carried out on the effect of implementing these regulations on their impact on companies, especially banking companies. There are several risks faced by banks. This risk is a reputation risk which can affect the liquidity of the banking system which will lead to the financial performance of the bank.

The target population in this study are banking companies listed on the Indonesia Stock Exchange. Banking companies are one of the companies that can play an active role in preventing money laundering. Almost all financial transactions are carried out by banks, so it can be said that they are the central figures in preventing money laundering. This study uses a population of banking companies listed on the Indonesia Stock Exchange because the researcher focuses on banking companies that are known by the wider community with a wide reach, large number of customers and large managed funds.

2. Literature review

2.1 *Factors causing money laundering*

There are several factors that cause money laundering crimes. First, in the crime of money laundering, there are several steps that are passed. The first is a placement, where in this phase the funds or cash derived from illegal transactions enter the financial system, which in this case enters the banking system. Many media that can be done such as cash deposits. Then after placement enter the layering (transfer) phase where in this phase the funds from the illegal transactions or what is commonly called dirty money have entered the financial system and can be done for financial transactions, in this phase the funds will move around to deceive origins. proposal of the fund. Then enter the final phase, namely Integration (integration) where the funds are ready to be used for things or objects that seem halal or commonly called clean money so that they can continue again for matters related to money laundering such as buying assets and opening effort (Abu Olaim & Rahman, 2016; He, 2010; Nobanee & Ellili, 2018; Ping, 2004).

Money laundering starts with dirty money or commonly referred to as dirty money or in Indonesia it is often called haram money. According to Sarah N. Welling, there are two ways to get dirty money, the first is through tax evasion, which is done by many corporations in the world. In terms of tax evasion, the company actually gets halal or clean results, not through illegal business activities but when reporting to regulators, especially in tax reporting so that tax payments are less than they should be. Then the second comes from business activities that are indeed illegal, which violates the law such as the sale of illegal drugs, gambling, bribery, and prostitution. In the PPATK regulations, there are many types of prohibited business activities or illegal business actions.

According to Nair and Vaithilingam (2007) there are several factors that influence money laundering. Several influencing factors include infrastructure, intellectual capital, institutions, integrity, and innovation.

One of the influencing factors is infrastructure, which is meant here in the crime of money laundering is the need for media to do this, such as the internet network and access to transact internationally. With the media or infrastructure, it can make it easier for the dirty money to travel to institutions or institutions for layering.

Technium Social Sciences Journal
Vol. 37, 287-299, November, 2022
ISSN: 2668-7798
www.techniumscience.com

Then another factor is intellectual capital, where the knowledge of a bank official is one of the keys where the employee understands the ins and outs of the bank and is a person who understands banking products well. So that with the ability or skill possessed and with the information at hand, it will be easy to commit fraud both from within and from within the bank, as well as assisting external parties to commit fraud.

Next is the institution in question is the legal and regulatory framework, where there have been many studies such as those conducted by (Abu Olaim & Rahman, 2016; He, 2010; Nobanee & Ellili, 2018; Ping, 2004). About that. In this case the regulation is one of the fences or boundaries that must be obeyed by banks so as to minimize the occurrence of fraud. At least you have been able to select from the placement phase so you can't proceed to the next stage.

Then next is the governance system, where a good corporate governance system can be implemented in accordance with applicable regulations. With good governance, it is hoped that there will be good implementation within the company. With good implementation, it is hoped that there will be internal protection within the company.

2.2 *Anti-money laundering disclosure*

In international relations, there is an index that measures the crime of money laundering. This index was compiled by the Basel Institute which consists of five categories and 14 indicators that identify a country's risk profile regarding money laundering and terrorism financing. In preparing the index, Basel did not move by itself but complied with the rules or recommendations of the Financial Action Task Force (FATF).

In the index developed by Basel, they did not create the data themselves but took information from various sources such as the FATF, the World Bank, and the World economic forum (Nobanee & Ellili, 2018). This index measures the overall risk of a country. The limitation in using the Basel AML index is that it only measures a country's risk not to financial institutions or corporations.

In this study, the researcher developed an index that had previously been developed by Nobanee & Ellili (2018) where the index has been adjusted so that it can be seen from the company's financial statements and websites of the companies studied. The AML Index developed by Nobanee & Ellili (2018) has 6 dimensions, in which there are 55 indicators in the 6 dimensions. These dimensions include (1) general anti-money laundering information, (2) statistics and reports, (3) know your customer, (4) risk assessments, (5) transaction monitoring and investigations, (6) technology. The researcher added 3 indicators in this study, 2 indicators in the know your customer dimension and 1 indicator in transactions monitoring and investigations, bringing the total indicators to 58 indicators.

In the research conducted by Nobanee & Ellili (2018), there are still shortcomings which have not included the element of employee due diligence where fraud is not only from external banking factors but can also come from internal companies. There have been several cases in Indonesia involving employees from these banks. In addition, along with the development of the times, many fintech companies have emerged where these companies must be monitored properly which has not been found in previous research.

Technium Social Sciences Journal
Vol. 37, 287-299, November, 2022
ISSN: 2668-7798
www.techniumscience.com

In the know your customer dimension, the researcher added 2 indicators, namely employee due diligence (EDD) and verification of customer financial technology. It can be realized that fraud is not only from external factors of the bank, but many cases also occur which originate from the bank's internal. Moreover, there is cooperation between external and internal parties of the bank which is a trigger factor for greater fraud. There are several major cases originating from internal banking, such as the case experienced by Citibank with Melinda dee as the suspect. Thus the assessment of banking employees must be one of the important factors in preventing fraud.

In addition, the researchers also added verification of financial technology customers, where currently many fintech companies have started to appear, reported from the kompasiana news site, in 2015 the fintech association was established and the number of fintech start-ups registered with the Financial Services Authority (OJK) rose to 111 companies in September 2016 from the position of April 2016 which was only 60 companies. Because regulations regarding fintech are not as stringent as banking regulations, it is expected to avoid the layering process of the money laundering process through fintech start-up companies.

Then in the dimensions of transactions monitoring and investigations, the researcher adds a cash basis transactions monitoring indicator, this is to prevent money laundering from the placement phase, in addition to the large number of hand arrest operations carried out by the KPK which is an indication that many money laundering transactions are carried out with cash transactions.

2.3 *Cyber security*

In addition to intellectual capital, one of the factors that support the success of a bank is the security system of the bank. We have entered the digital era where almost every service is done digitally. Especially in the banking industry starting from phone banking, sms banking, internet banking to mobile banking. Almost all of these media can fulfill customer transaction activities such as transferring funds, paying bills, and placing deposits. For daily transaction needs, it can be accessed through a gadget that is carried anywhere every day, there is no need to come to the nearest branch or atm, atm is only visited if you want to make cash withdrawals. The rest is to increase the e-wallet balance with the gadgets you have.

According to (El-Bannany, 2008) in general, information technology systems can be classified into two groups, namely systems for internal companies such as systems for document storage, management information systems used by company managers. And the second is a system for external companies such as internet banking and ATM networks.

Internet banking is one of the fastest and easiest ways to do banking transactions. The threat from cyber security is also a formidable challenge in this digital era. There are 2 aspects from the user's point of view, the first is how customers conduct transactions through internet banking and the second is the awareness of users of threats that may arise in the future. There are several responses where the user's lack of awareness of cyber threats is the main reason for fraud. It is hoped that the bank will play an active role in making the public aware of the threats in online financial transactions (Alghazo & Kazmi, 2017).

There are various threats that often occur in online transactions such as phishing, social engineering. In phishing mode the user is made to appear to provide confidential information through the system they are doing. While in social engineering, users are tricked through words

Technium Social Sciences Journal
Vol. 37, 287-299, November, 2022
ISSN: 2668-7798
www.techniumscience.com

spoken by fraudsters either by telephone or other means of communication (Alghazo & Kazmi, 2017; Dhanalakshmi et al., 2011; Dodge et al., 2007; Gan et al., 2008; Workman, 2007).

3. Data and methodology

3.1 *Data*

In this study, the purpose of this study is to test the hypothesis to analyze the effect of the variable AML disclosure and cyber security on bank performance. The objects that are the focus of this research are Anti Money Laundering (AML) disclosure, cyber security, and Bank Performance in banking companies listed on the Indonesian stock exchange.

In this study, the sample used is banking companies listed on the Indonesia Stock Exchange (IDX) which publish financial reports along with annual reports from 2016 to 2020.

3.2 *Methodology*

In this study, the population used is banking companies listed on the Indonesia Stock Exchange (IDX) in 2016-2020. Sampling was done by purposive sampling method, which means that the sample must be in accordance with the criteria that have been set in order to get a sample that fits the needs of this study.

The data used in this study uses secondary data obtained from financial statements, obtained from the Indonesian Stock Exchange Capital Market Reference Center. Annual financial reports are published by companies listed on the IDX, the Indonesia Capital Market Directory (ICMD), the IDX website at www.idx.co.id and from internet sites.

4. Empirical result

Variabel	**Prediction**	***Coefficient***	***Sig.***
C		3,987838	0,0000
AML	+	0,000572	0,0287*
CS	+	-0,004414	0,0035*
IC	+	3,25E-06	0,0345*
AML*IC	+	-1,34E-07	0,0318*
CS*IC	+	2,96E-06	0,0005*
KA		0,000134	0,0038*
SIZE		-2,29E-05	0,9733

4.1 *Discussion of the Effect of Anti Money Laundering (AML) Disclosure on Bank Performance.*

The results of the t test show that there is an effect of Anti Money Laundering (AML) Disclosure on Bank Performance. These results prove that partially Anti Money Laundering (AML) Disclosure affects the Bank Performance variable. The coefficient of the Anti Money Laundering (AML) Disclosure variable which is positive at 0.000572 also supports the research

theory which states that Anti Money Laundering (AML) Disclosure has a positive effect on Bank Performance. From these results, Hypothesis one (H1) can be accepted and H0 is rejected so that it is concluded that Anti Money Laundering (AML) Disclosure has a positive and significant effect on Bank Performance. Answering research questions based on the results of the t-test answers research questions that AML disclosure has a positive effect on bank performance.

Based on the signal theory that AML disclosure is a signal where the signal indirectly affects the reputation of the banking company where with the disclosure, the bank is considered more transparent to stakeholders. With a good bank reputation, the bank has a low reputation risk. With a low reputation risk, it is expected that public confidence in banks will be high which will have an impact on the level of banking liquidity. With a high level of liquidity, it has high managed funds so that it can improve the performance of the banking company itself.

The results of this study do not agree with the research conducted by (Nobanee and Ellili, 2018) which found that AML disclosure had no effect on the performance of banking companies. It was stated in previous research that the low disclosure of money laundering did not affect banking companies in the UAE.

4.2 *Discussion of the Effect of Cyber Security (CS) on Bank Performance.*

The results of the t-test found that there was no positive effect of Cyber Security (CS) on Bank Performance. These results prove that partially Cyber Security (CS) does not affect the Bank Performance variable. The variable coefficient of Cyber Security (CS) which is negative at -0.004414 also does not support the theoretical research which states that Cyber Security (CS) has a positive effect on Bank Performance. From these results, Hypothesis two (H2) cannot be accepted and H0 is accepted so that it can be concluded that Cyber Security has no positive effect on Bank Performance.

Referring to the agency theory, the bank and the customer have their respective roles in maintaining the security of banking transactions. Where the bank's internal system needs to be maintained because it is needed for monitoring transactions and information for employees and management while the external system is a service that can be enjoyed by the bank's customers. In a previous study conducted by Campbell et. al. (2003) investigated the stock market reaction in public companies when there was information on cyber attacks and there was no significant effect, this is because the difference in information leaked has different results in its impact on the stock market reaction. Currently, some people are still focused on the products offered by banks in the form of ease of access to services offered by banks, besides that public literacy related to cyber security can be said to be still minimal so that it has not affected the company's performance.

The results of this study do not agree with the research conducted by M. Ko, C. Dorantes (2006) that if there is a cyber security threat, financial performance will decrease. This is due to the additional costs that must be paid by the company, resulting in a decrease in the company's financial performance. In addition, previous research explained that if there is an attack on information technology, the company will experience a decrease in market value by 2.1% in the next 2 days Cavusoglu et al (2004).

Technium Social Sciences Journal
Vol. 37, 287-299, November, 2022
ISSN: 2668-7798
www.techniumscience.com

4.3 *Intellectual capital discussion strengthens the influence of AML disclosure on Bank Performance.*

The results of the t test found that Intellectual Capital did not strengthen the effect of Anti Money Laundering (AML) Disclosure on Bank Performance. These results prove that partially Intellectual Capital cannot moderate the effect of the Anti Money Laundering (AML) Disclosure variable on the Bank Performance variable. The coefficient of the Anti Money Laundering (AML) Disclosure variable moderated by Intellectual Capital is negative at -1.34E-07 nor does it support the research theory which states that Intellectual capital strengthens the influence of AML disclosure on Bank Performance. From these results, hypothesis three (H3) cannot be accepted and H0 is accepted so that it is concluded that Intellectual capital does not strengthen the influence of AML disclosure on Bank Performance.

The results of this test are not in accordance with signal theory where with good intellectual capital the bank will be more compliant with regulations, the bank will have good transparency in the eyes of the stakeholders. From the test results that intellectual capital does not strengthen the influence of AML disclosure on bank performance, this is because there is still a lack of education related to AML so it is necessary to increase knowledge about AML regulations so that banks will be more transparent.

In a previous study conducted by M. Simwayi, G. Wang (2011) that the lack of knowledge of employees who work in the AML work unit, the result is that the bank's compliance with AML regulations is also low. This is due to the lack of knowledge of the work unit employees with applicable regulations. To improve this, it is necessary to have support from management to increase the knowledge of the employees who work in the unit.

4.4 *The discussion of Intellectual capital strengthens the influence of Cyber security on Bank Performance.*

The results of the t-test found that Intellectual Capital strengthens the effect of Cyber security on Bank Performance. These results prove that partially Intellectual Capital can moderate the influence between Cyber security variables on Bank Performance variables. The coefficient of Cyber security variable moderated by Intellectual Capital is positive at 2.96E-06 which also supports the theoretical research which states that Intellectual capital strengthens the influence of Cyber security on Bank Performance. From these results, hypothesis four (H4) can be accepted and H0 is rejected so that it is concluded that Intellectual capital strengthens the influence of cyber security on Bank Performance.

Referring to signal theory, with the high investment in cyber security and the presence of qualified human resources, it is hoped that the technology can be optimized so as to improve company performance. With the help of technology and efficient human resources, banks can perform operational efficiency and can improve company performance.

This study does not agree with previous research conducted by El-Banany (2008) that IT investment has a negative effect on intellectual capital. This is because a large investment in technology will threaten the workforce so that labor can be replaced by technology, so there can be a reduction in employees in bank operations such as a reduced number of bank tellers.

Technium Social Sciences Journal
Vol. 37, 287-299, November, 2022
ISSN: 2668-7798
www.techniumscience.com

5. Conclusion

From the results of the Anti-money laundering (AML) test, the disclosure has a positive effect on bank performance. The results of this study are in accordance with the signaling theory where with the disclosure of AML disclosure, the bank is considered more transparent so that it can improve the reputation of the bank and attract the attention of the public. With a good reputation, banking liquidity will be greater so that it can improve company performance. In the future, it is expected that banks will compete to increase transparency through voluntary disclosure, especially in this study, disclosures related to AML disclosure. This research can be a reference for banks to increase transparency in order to improve the reputation of the bank.

From the test results also found that cyber security has no effect on bank performance. Cyber security can be divided into two parts, between the system used by the internal bank and the external bank. Internal functions are used for bank employees and management to monitor banking activities, while external functions are used for customers to conduct banking transactions. Security in transactions has not become a priority for customers because currently there are many kinds of digital banks that facilitate many banking service products. Currently, some customers are still focused on banking services that can be enjoyed so that cyber security does not affect bank performance.

The results of intellectual capital testing do not moderate AML disclosure on bank performance. This is not in accordance with signal theory where with good intellectual capital, banks will be more compliant with regulations, banks will have good transparency in the eyes of stakeholders. From the test results that intellectual capital does not strengthen the influence of AML disclosure on bank performance, this is because there is still a lack of education related to AML so it is necessary to increase knowledge about AML regulations so that banks will be more transparent. AML units need special training and AML education not only for employees who work only in these units but also for all banking employees and also for education to prospective customers.

The results of the test found that intellectual capital moderates cyber security on bank performance. Referring to signal theory, with the high investment in cyber security and the presence of qualified human resources, it is hoped that the technology can be optimized so as to improve company performance. With the help of technology and efficient human resources, banks can perform operational efficiency and can improve company performance.

There are regulations related to money laundering issued by the financial services authority, namely POJK No. 23 /POJK.01/2019 concerning the implementation of anti-money laundering and prevention of terrorism financing programs in the financial services sector. The regulation contains guidelines on how to monitor and programs that must be implemented to prevent money laundering and terrorism financing. The regulation also contains matters that need to be reported to the regulator related to the programs that have been implemented. If possible, the regulator can add reporting on the implementation of the program in order to convey information and transparency to stakeholders.

References

[1] Rahman, A. (2014). Combating money laundering and the future of banking secrecy laws in Malaysia. *Journal of Money Laundering Control*, *17*(2), 219–229. https://doi.org/10.1108/JMLC-09-2013-0036

[2] Abu Olaim, A. M. A., & Rahman, A. A. (2016). The impact of Jordanian anti-money laundering laws on banks. *Journal of Money Laundering Control*, *19*(1), 70–78. https://doi.org/10.1108/JMLC-07-2014-0023

[3] Al-hajaya, K., Altarawneh, M. S., & Altarawneh, B. (2019). Intellectual Capital Disclosure by Listed Companies in Jordan : A Comparative Inter-sector Analysis. *International Review of Management and Marketing*, *9*(1), 109–116.

[4] Alghazo, J. M., & Kazmi, Z. (2017). *Cyber Security Analysis of Internet Banking in Emerging Countries : User and Bank Perspectives*.

[5] Ali, H.M. and Ahmad, N.H. (2006), "Knowledge management in Malaysian banks: a new paradigm", JournalofKnowledgeManagementPractice,Vol.7No.3,pp.1-13.

[6] Ballina, F. J., Valdés, L., & Valle, E. Del. (2019). The Signalling Theory : The Key Role of Quality Standards in the Hotels Performance The Signalling Theory : The Key Role of Quality Standards. *Journal of Quality Assurance in Hospitality & Tourism*, *0*(0), 1–19. https://doi.org/10.1080/1528008X.2019.1633722

[7] Bidabad, B. (2017). Money laundering detection system (MLD) (a complementary system of Rastin banking). *Journal of Money Laundering Control*, *20*(4), 354–366. https://doi.org/10.1108/JMLC-04-2016-0016

[8] Campanella, F. (2014), "Assess the rating of SMEs by using classification and regression trees (CART) withqualitativevariables",ReviewofEconomics&Finance,Vol.4No.3,pp.16-32.

[9] Chaikin, D. (2008). Commercial corruption and money laundering: a preliminary analysis. *Journal of Financial Crime*, *15*(3), 269–281. https://doi.org/10.1108/13590790810882865

[10] Cheng, L. and Leong, S. (2017), "Knowledge management ecological approach: a cross-discipline case study",JournalofKnowledgeManagement,Vol.21No.4,pp.839-856.

[11] Connelly, B. L., Certo, S. T., Ireland, D., & Reutzel, C. R. (2010). Signaling theory: A review and assessment. *Journal of Management*, *37*(1), 39–67. https://doi.org/10.1177/0149206310388419

[12] Cross, R. and and Weller, S. (2001), "Winning through knowledge (knowledge management in banks)", FinancialWorld,p.19.

[13] Curado, C. (2008), "Perceptions of knowledge management and intellectual capital in the banking industry",JournalofKnowledgeManagement,Vol.12No.3,pp.141-155.

[14] Daily, C. M., Dalton, D. R., & Rajagopalan, N. (2003). Governance through ownership: Centuries of practice, decades of research. *Academy of Management Journal*, *46*(2), 151–158. https://doi.org/10.2307/30040611

[15] Dalwai, T., & Mohammadi, S. S. (2020). Intellectual capital and corporate governance: an evaluation of Oman's financial sector companies. *Journal of Intellectual Capital*, *21*(6), 1125–1152. https://doi.org/10.1108/JIC-09-2018-0151

[16] DelGiudice,M.,Campanella,F.andDezi,L.(2016),"The bank of things: an empirical investigation on the profitability of the financial services of the future", Business Process Management Journal, Vol. 22, No. 2, pp.324-340
[17] Dhanalakshmi, R., Prabhu, C., & Chellapan, C. (2011). Detection Of Phishing Websites And Secure Transactions. *Detection Of Phishing Websites And Secure Transactions International Journal Communication & Network Security*, *Ii*.
[18] Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers and Security*, *26*(1), 73–80. https://doi.org/10.1016/j.cose.2006.10.009
[19] El-bannany, M. (2008). *A study of determinants of intellectual capital performance in banks : the UK case*. *9*(3), 487–498. https://doi.org/10.1108/14691930810892045
[20] Gan, G. G. G., Ling, T. N., Yih, G. C., & Eze, U. C. (2008). Phishing: A growing challenge for internet banking providers in Malaysia. *Innovation and Knowledge Management in Business Globalization: Theory and Practice - Proceedings of the 10th International Business Information Management Association Conference*, *1–2*, 1276–1285.
[21] Haniffa and Hudaib. (2006). *Corporate Governance Structure and Performance of Malaysian Listed Companies*. *33*(October), 1034–1062. https://doi.org/10.1111/j.1468-5957.2006.00594.x
[22] He, P. (2010). *A typological study on money laundering*. *13*(1), 15–32. https://doi.org/10.1108/13685201011010182
[23] Ho, C., & Williams, S. M. (2003). *International comparative analysis of the association between board structure and the efficiency of value added by a firm from its physical capital and intellectual capital resources*. *38*, 465–491. https://doi.org/10.1016/j.intacc.2003.09.001
[24] Irwin, A. S. M., Slay, J., Raymond Choo, K. K., & Lui, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. *Journal of Money Laundering Control*, *17*(1), 50–75. https://doi.org/10.1108/JMLC-06-2013-0019
[25] Jayasundara, C. (2008), "Knowledge management in banking industries: uses and opportunities", JournaloftheUniversityLibrariansAssociationofSriLanka,Vol.12,p.12
[26] Jensen, M. C., & Meckling, W. H. (1976). Theory of the Firm: Managerial. *Journal of Financial Economics*, *3*, 305–360. https://doi.org/http://dx.doi.org/10.1016/0304-405X(76)90026-X
[27] Kapopoulos, P., & Lazaretou, S. (2007). *Corporate Ownership Structure and Firm Performance : evidence from Greek firms*. *15*(2), 144–158.
[28] Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, *17*(2), 13–22.
[29] Krivogorsky, V. (2006). *Ownership , board structure , and performance in continental Europe*. *41*, 176– 197. https://doi.org/10.1016/j.intacc.2006.04.002
[30] Le Nguyen, C. (2014). The international anti-money laundering regime and its adoption by Vietnam. *Asian Journal of International Law*, *4*(1), 197–225. https://doi.org/10.1017/S2044251313000349
[31] Lu, X., & White, H. (2014). Robustness checks and robustness tests in applied economics. *Journal of Econometrics*, *178*(PART 1), 194–206. https://doi.org/10.1016/j.jeconom.2013.08.016
[32] Mavridis & Kyrmizoglou. (2005). *In tel lec tual Cap i tal Per for mance Driv ers in the Greek Bank ing Sector*.

[33] Nantapanuwat, N., Ractham, P. and Kaewkittipong, L. (2010), "An investigation of the determinants of knowledge management systems success in banking industry", International Journal of Economics and ManagementEngineering,Vol.4No.11,pp.588-595.
[34] Nobanee and Ellili. (2018). Anti-money laundering disclosures and banks ' performance. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-10-2016-0063
[35] Nobanee, H., & Ellili, N. (2018). Anti-money laundering disclosures and banks' performance. *Journal of Financial Crime*, *25*(1), 95–108. https://doi.org/10.1108/JFC-10-2016-0063
[36] Orazalin, N., Mahmood, M., & Lee, K. J. (2016). *Corporate governance , financial crises and bank performance : lessons from top Russian banks*. https://doi.org/10.1108/CG-10-2015-0145
[37] Panda, B., & Leepsa, N. M. (2017). Agency theory: Review of theory and evidence on problems and perspectives. *Indian Journal of Corporate Governance*, *10*(1), 74–95. https://doi.org/10.1177/0974686217701467
[38] Ping, H. (2004). Banking secrecy and money laundering. *Journal of Money Laundering Control*, *7*(4), 376–382. https://doi.org/10.1108/13685200410810074
[39] Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security? *Journal of Intellectual Capital*, *20*(5), 621–641. https://doi.org/10.1108/JIC-04-2019-0079
[40] Saengchan, S. (2008), "The role of intellectual capital in creating value in the banking industry", InternationalReviewofBusinessResearch,Vol.7No.2,pp.157-169
[41] Samantha Maitland Irwin, A., Raymond Choo, K. K., & Liu, L. (2011). An analysis of money laundering and terrorism financing typologies. *Journal of Money Laundering Control*, *15*(1), 85–111. https://doi.org/10.1108/13685201211194745
[42] Simwayi, M., & Wang, G. (2012). *The role of money laundering reporting officers in combating money laundering in Zambia*. https://doi.org/10.1108/15285811111172303
[43] Sorrentino, M. (1999),"Notes on knowledge managementin banking", KIO Meeting, Barcelona,available at:www.sistemi-informativi.org/kio/cons/KIOme&BarRTF.htm
[44] Teichmann, F. M. J. (2017). Twelve methods of money laundering. *Journal of Money Laundering Control*, *20*(2), 130–137. https://doi.org/10.1108/JMLC-05-2016-0018
[45] Vaithilingam, S., & Nair, M. (2007). Factors affecting money laundering: lesson for developing countries. *Journal of Money Laundering Control*, *10*(3), 352–366. https://doi.org/10.1108/13685200710763506
[46] Wang, W. K., Lu, W. M., & Lin, Y. L. (2012). Does corporate governance play an important role in BHC performance? Evidence from the U.S. *Economic Modelling*, *29*(3), 751–760. https://doi.org/10.1016/j.econmod.2012.01.021
[47] Williams, T. F. (2009). Banker as victim: an approach to money laundering prosecutions. *Journal of Money Laundering Control*, *12*(1), 50–58. https://doi.org/10.1108/13685200910922642
[48] Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, *16*(6), 315–331. https://doi.org/10.1080/10658980701788165
[49] Young, M. A. (2013). The exploitation of offshore financial centres: Banking confidentiality and money laundering. *Journal of Money Laundering Control*, *16*(3), 198–208. https://doi.org/10.1108/JMLC-01-2013-0004

Technium Social Sciences Journal
Vol. 37, 287-299, November, 2022
ISSN: 2668-7798
www.techniumscience.com

[50] Zolkaflil, S., Omar, N., & Syed Mustapha Nazri, S. N. F. (2019). Implementation evaluation: a future direction in money laundering investigation. *Journal of Money Laundering Control*, *22*(2), 318–326. https://doi.org/10.1108/JMLC-03-2018-0024