International Journal of Economics and Finance; Vol. 11, No. 10; 2019
ISSN 1916-971X E-ISSN 1916-9728
Published by Canadian Center of Science and Education

Cyber Laundering: A Threat to Banking Industries in Bangladesh: In Quest of Effective Legal Framework and Cyber Security of Financial Information

Nahid Joveda[1], Md. Tarek Khan[2] & Abhijit Pathak[2]

[1] Faculty of Business Administration, BGC Trust University Bangladesh, Chandanaish, Chattogram, Bangladesh

[2] Department of Computer Science and Engineering, BGC Trust University Bangladesh, Chandanaish, Chattogram, Bangladesh

Correspondence: Nahid Joveda, Faculty of Business Administration, BGC Trust University Bangladesh, Chandanaish, Chattogram-4381, Bangladesh. Tel: 019-1701-8610. E-mail: nahidjoveda87@gmail.com

Received: August 19, 2019 Accepted: September 6, 2019 Online Published: September 17, 2019

doi:10.5539/ijef.v11n10p54 URL: https://doi.org/10.5539/ijef.v11n10p54

Abstract

Cyberspace is a great media for exchanging information and data in the arena of E-banking. Banks are under pressure for the establishment of digitalization in its day by day operations to satisfy the clients' need. But the abuse of information technology has become a menace in the banking sector of Bangladesh. Concealing of original source and using advance technological solutions to transfer money illegally– the whole phenomenon is called Cyber laundering. This paper offers insights to increase an understanding of the nexus of corruption in banks, local economy and money laundering scandals. It examines the launderers' typology of crimes— both potential and real. Through this paper it is a small initiative to point out the national control mechanisms to deal with the issues of money laundering in banks. The research is based on accessible data from papers, journals, various reports, etc. The illicit flow of money through banks has created worldwide millions of dollar misfortunes. This paper focuses on creating a Cybersecurity system for detecting money laundering as it has become a threat to Bangladesh's economy. Are there any self-evident weaknesses in the financial framework that make it treatable efficiently? It is critical to acknowledge that how the security viewpoints in a financial framework can impact such unlawful exercises which are then lead to an extraordinary lost to the economic development.

Keywords: banking sector, cyber laundering; control mechanism, cybersecurity protocol, trade-based laundering, AML

1. Introduction

The outset of money laundering has been found in the nineteenth century. On that time money laundering was done by robbers and pirates. As time passes money laundering concept also changed. Advancement of technology and financial globalization makes easier to transfer funds illegally and then the term cyber laundering has emerged. Cyber laundering is the practice of money laundering carried out in cyberspace through online transactions. Launderers use a diverse and innovative method for concealing and expose financial institutions or banks to legal risk, reputation risk, operational risk, and financial risk.

Cyber laundering has become a burning issue and different international organizations, law execution agencies, financial intelligence units, etc. are working to prevent laundering worldwide. According to the Swiss National Bank data deposit of Bangladeshi people rises from 4064 crores in 2017 to 5341 crores in 2018. Big chunk of money goes out of the country every year and offshore companies are another reason identified by the Center for Policy Dialog. The Panama Papers have identified 50 Bangladeshi citizens who launder money to avoid tax. Bangladesh Institute of Bank The management research report shows that 4% of banks have employees with outstanding knowledge about IT, 28% are unaware while 20% of officials have a poor knowledge. The forces that make Cybersecurity complicated are- use of third-party merchants, evolving classy technologies, cross-border data exchanges, increased use of mobile technology and the adoption of the Internet of Things (IoT). Bangladesh is in such an ailment where banks must confiscate any gap available in ensuring information security.

This paper starts with analyzing the existing literature on money laundering and Cybersecurity issues. Then the process of cyber laundering within the context of Bangladesh has been discussed elaborately. The following part describes the impact of cyber laundering on Bangladesh economy and different control mechanism adopted by anti-money laundering professional bodies. This study shows the major incidents of laundering in banks and a cyber-security system was developed to detect cyber laundering in banks. Implementing this new concept will help us promote a strong anti-money laundering environment to prevent financial crime.

Money launderers are unpredictable, and they are using different techniques to transfer money illegally. But the whole process consists of three stages that are summarized with the help of the following table:

Table 1. Stages of money laundering.

Stages of Money Laundering

SOURCES OF INCOME	PLACEMENT	LAYERING	INTEGRATION
	Deposit Unlawful proceeds Into Financial System	Conceal the Criminal Origin of Proceeds	Create a Deceptive Legal Origin for Criminal Proceeds
• Tax Crimes • Fraud • Embezzlement • Drugs • Theft • Bribery Corruption	• Change of Currency • Change of Denominations • Transference of Cash • Cash Deposits	• Wire Transfers • Withdrawals in Cash • Cash Deposits in other Bank Accounts • Split and Merge between Bank Accounts	• Creating Fictitious Loans, Turnover/'Sales, Capital Gains, Deeds. Contracts, Financial Statements • Disguise Possession of Assets • Illegal Funds Used in Third-party Transactions

2. Objectives

The study is focused to achieve the following objectives:

- To explore the real phenomenon of cyber laundering in the banking sector of Bangladesh.
- To examine the domestic anti-money laundering control measures are taken by the professional bodies.
- To demonstrate the special effects of money laundering in the Bangladesh economy and the major heists through money laundering in recent years.
- To propose a unique Cybersecurity system to detect money laundering in banks.

3. Methodology of the Study

The study is descriptive. This study is conducted based on secondary data. The data was collected from the circulars of Bangladesh Bank, different reports, research papers from various journals, local newspapers, websites, etc. to develop the theoretical framework of the study. Data of Basel Anti-Money Laundering Index of the last five (2014-2018) years have been collected to show comparative trend analysis among South Asian Countries including Bangladesh.

4. Limitations of the Study

The main limitation of the study is the availability of quality data measuring the patterns of money laundering over the specific period. Apparently conducting research on laundering activity poses a great challenge because launderers and their banks don't share any information regarding their unlawful activities. Moreover, there is no exact mechanism to detect money laundering when it happened. Besides this, there is no quantitative model to define money laundering and to solve it.

5. Literature Review

Money Laundering is comparatively a contemporary topic within the context of Bangladesh. Hence, there's a scope for locating new trends supported experiences of jurisdictions that have enforced their opposed concealing framework. This is often necessary from the legislative purpose and the attitude of the economic sector and financial markets. A review of the literature on the market within the field reveals the subsequent observations still as potential gaps, that a additional underline the importance of analysis during this regard:

EAG (2013) "Typology Report on money laundering Through the Security Markets" has counseled entomb Alia

that jurisdictions that haven't selected stock exchange offences viz. swapping, market manipulation, and securities-related fraud as ML/TF offences could create mandatory changes in their laws to incorporate the identical.

FATF (2013) Report on "The Role of Hawala and other Similar Service suppliers (HOSSPs) in concealing and Terrorist Financing" concludes that effective superintendence of HOSSPs is one among the first challenges facing regulators and their Governments. The International community will address the ensuing vulnerability by transportation the HOSSPs underneath risk-based AML/CFT restrictive and super ordinate framework that's effectively enforced.

Sultana Sharmeen Karim (2016) emphasized on evolving a conceptual framework regarding the issues of cyber-crime in the banking sector of Bangladesh. She focused on the concept of the basic crimes happened in banks and the financial sector- namely Automated Teller Machine (ATM) frauds, E-Money Laundering, etc. She suggests that by applying the modernized technology and appointing skilled human resources and devices cyber-crime can be minimized from the banking transactions.

Akin Olawale (2016) revealed in their study, various effects of money laundering such as economic effect, political effect, financial effect, etc. They suggested harmonizing laws on money laundering and to increase punishment.

Saiful, Akter, and Zahed (2017) found that predicate offences of money laundering can be lessened mostly through examining the doings of local criminals with foreign network and strong anti-corruption measures through automation in National Board of Revenue. They also provided information about the position of Bangladesh in case of money laundering in the Basel AML Index Score.

Moh Zali and Ach Maulidi (2018) focused on the establishment of the conspiracy theory of a crime that includes the deterrence effect in the respect of perpetrators such as dishonest local business staff, corrupter and launderers. They also suggest that the enforcement of money laundering laws and creation of anti-money laundering agencies that can effectively deter greedy activities of financial intermediaries in helping money laundering practices.

Ricky Leung (2018) focused on the Cybersecurity regulations in the UK, USA, Hong Kong, and Singapore. He also suggests for consumer banks running online banking systems, educating customers about the basics of mitigating Cybersecurity risks are arguably at least as important as ensuring the systems, controls, and processes on the side of the bank are sufficiently resilient.

"Majority of banks still vulnerable to cyber-attacks" a report was published in Dhaka Tribune dated February 05, 2018. It shows that on January 06, 2013 website of Islami Bank Bangladesh Limited was hacked by the Tunisian hacker Human Mind Cracker, on December 02, 2015 Hacker KinGnCa breached the Sonali Bank's network security and took control of the website, in February 2016 ATM booths of Dutch-Bangla Bank Limited, City Bank, Trust Bank limited was hacked.

6. Money Laundering in the Context of Bangladesh

Money laundering has become a pressing issue for the economy of Bangladesh. One of the reasons for money laundering be tax evasion. It decreases tax revenue of the government and creates an extra burden on the honest taxpayers. It has severe economic effect as a huge amount of money invested in crime activities, therefore, income inequality increases. If money is transferred to abroad then ultimately it reduces national reserve. Corruption in banks which lead to laundering money creates debasement to the reputation and trust of banks.

6.1 Reasons for Cyber Laundering

There are some reasons why money laundering happens-

- The fundamental reason behind concealing in Bangladesh is the evasion of tax.
- Lack of political transparency and smart governance that has created and inspired corruption altogether sectors of the society.
- Big informal employment and unthinkably high informal dealing within the economy that left a lot of undefined sources.
- Political instability could be a major concern for the material resource that somehow compels them to appear for an external destination.

6.2 Who Are the Launderers?

Each year a large volume of money continues to be siphoned off as the Anti-money Laundering Act and

Cybersecurity system appears inadequate in deterring capital flight in Bangladesh. Steinko and Tilley Hopkins suggests that International laundering of money is often not to do by the same persons who connect in criminal and illegal activities but by experts who are well-known with the workings of international capital markets and who are thus able to determine the risks of detection and to exploit differences in controls and regulations among countries. Money laundering is done by ruling party men, government blessed businessmen and top bureaucrats in Bangladesh. Sometimes it is done by collusion between importers, exporters and bank officials. Drug traders, smugglers, terrorists, illegal arms dealers, corrupted private and public officials are also involved in money laundering.

6.3 Offences of Money Laundering

The Bangladesh Parliament approved the Money Laundering Prevention Act in February 2012. Major crimes that may affect the country's financial system under the MLP Act, 2012 are as follows: (a) corruption and corruption (b) counterfeiting of currency, (c) counterfeiting of papers (d) fraud and forgery (e) illegal trafficking of firearms (f) illicit trafficking of narcotic drugs (g) illicit trafficking of stolen and other products (h) snatching, illegal confinement and hostage-taking I murder, serious physical injury (j) black marketing, k) national and foreign currency trafficking l) human trafficking m) customs and excise duty trafficking and offences n) tax offences, o) violation of intellectual property rights p) terrorism or terrorist financing q) insider trafficking and market manipulation using price-sensitive information r) any other offence declared by Bangladesh Bank as a predicate offence against Government.

6.4 Trade-Based Laundering in Banks

Trade-based laundering is the method by which criminals use a legitimate trade to camouflage their illegal earnings from unprincipled sources. According to the International Narcotics Control Board's strategy report, hundreds of billions of dollars are laundered every year through trade-based concealing worldwide. Centre for Policy Dialogue shows that 85-90% of laundering happens through foreign trade in Bangladesh. Some factors are responsible for the growth of trade-based money laundering in the country. The factors include unskilled bankers, lack of effective data communication network between the customs and banks, the dreadful connection of corrupted traders and bankers, and lack of digitalization.

6.4.1 How Manipulation Occurs

Trade based laundering happened mostly in four forms - over and under-invoicing, over and under shipment, multiple invoices, and falsely declared goods and services. Unethical traders can make either over invoice in case of import or under invoice in case of export which can be termed as transfer mispricing. Shipping documents are also deployed in a way either by delivery of short amount of commodities than actual invoice value or shipment of more goods than the actual value of the invoice. Besides these, an exporter may not send any goods at all, but, fake documents and certificate of origin, etc. presented to banks called "phantom shipment". Moreover, to launder funds issuing more than one invoice for the same international trade transaction. Employing several financial institutions to make these extra payments can further raise the level of complexity adjacent such transactions. An exporter may ship a comparatively low-priced good and misleadingly bill it as a more expensive item or an entirely unlike item. This creates inconsistency between what seems on the shipping and customs documents and what is shipped.

6.4.2 Effects

According to Global Financial Integrity report based on 148 developing countries Illicit Financial Flow, Bangladesh got the 30th position in the Asian States. Bangladesh has been lost $5.9 billion in 2015, $ 9.1 billion in 2014, and $9.66 billion in 2013, and $7.23 billion in 2012 for trade-based laundering. Bad intents of traders unpleasantly affect the economy as well as health, education and other development strategies of a country. They use the money in the extremist doings like militancy and arson attack, drug misuse and human-trafficking and many other offences.

7. Anti-Money Laundering Measures in Bangladesh

In line with worldwide organisations, Bangladesh has also taken several measures to avoid money laundering and combat terrorist financing and the explosion of weapons of mass destruction, taking into consideration their severe impact on the country.

Preventive Measures	Description
Founding Member of APG	Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been joining the annual plenary meeting since 1997. As a member of APG, Bangladesh is dedicated to implementing FATF's 40 recommendations. Bangladesh accommodated the 13th APG Typologies Workshop in 2010 and APG Annual Meeting of 2016.
Legal Framework	Bangladesh is the first country in South Asia that has passed the Money Laundering Prevention Act (MLPA) in 2002. To overcome the insufficiencies of the MLPA, 2002 and to reach the international standards Bangladesh enacted Money Laundering Prevention Ordinance (MLPO) in 2008 which was swapped by MLPA, 2009 by the parliament in 2009. In February 2012, Bangladesh re-enacted Money Laundering Prevention Act repealing MLPA, 2009, to resolve the shortcomings found in the Mutual Evaluation Report (MER). Money Laundering Prevention Rules, 2013 for the efficient execution of the law is outlined.
Central and Regional Taskforces	On January 27, 2002, the Government of Bangladesh set up a core and seven regional task force (Chittagong, Rajshahi, Bogra, Sylhet, Rangpur, Khulna, and Barisal) to avoid unlawful hundi activity, illegitimate fund flow, and money laundering in Bangladesh.
Anti-Money Laundering Department	Anti-Money Laundering Department (AMLD) was recognized in Bangladesh Bank in June 2002 which operated as the FIU of Bangladesh. It was the authority for receiving, examining and circulating Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs).
Bangladesh Financial Intelligence Unit	According to MLPA's provision, 2012 Bangladesh Financial Intelligence Unit (BFIU) was created to stop AMLD as a domestic core organization receiving, analyzing and disseminating STRs / SARs, CTRs and complaints. The responsibility for exchanging ML & TF data with its overseas counterparts has been allocated to BFIU. BFIU's primary goal is to create an effective system for AML, CFT & CPF prevention and operational autonomy has been granted.
National strategy for ML, TF & PF prevention	In April 2011, the NCC introduced the National Strategy for preventing Money Laundering and Combating Terrorism Financing, 2011-2013. The strategy identifies the specific action plan to develop an effective AML & CFT system in Bangladesh for all ministries, divisions, and agencies. It consists of following 11 (eleven) strategies against 11 (eleven) strategic objectives: • Bring up-to-date National ML & TF Risk Assessment Report repeatedly and introducing a Risk-Based Approach of monitoring and supervision of all reporting organizations. • Discouraging corruption induced money laundering considering corruption as a danger. • Modernizing the Border Control Mechanism and depriving offenders of the use of criminal proceeds to avoid the smuggling of gold and drugs, trafficking in human beings, other transnational planned crimes taking into account the risk. • Tackling Illicit Financial Flows (IFF's) by stopping criminal earnings, curbing national and cross-border tax evasion and tackling money laundering based on trade. • Reforming the transfer of illicit funds by enhancing the speed of projects to recover stolen property and or recovering the tax evaded. • Improving BFIU's ability to identify and analyze emerging instances of ML & TF including hazards of ML & TF resulting from the use of new techniques. • Improve acquiescence with all reporting agencies with a particular focus on new reporting agencies such as NGOs / NPOs and DNFBPs. • Expand investigative ability and improve the quality of ML & TF cases inquiry and prosecution to deter criminals. • Effectively establishing TF & PF identification and monitoring mechanisms and completely implementing targeted TF & PF economic penalties. • Strengthening domestic and international policy and operational coordination. • Development in Bangladesh of a transparent, responsible and inclusive economic scheme.
Egmont Group Memberships	At the July 2013 Egmont Plenary in Sun City, South Africa, and BFIU entered the Egmont group. Through Egmont membership, BFIU has acquired entree to a wider universal stage and this will help to build affiliation with other FIUs from different countries to benefit from the exchange of views, experiences, and information through the Egmont Secure Web.
Memorandum of Understanding (MOU) Between ACC and BFIU	The Anti-Corruption Commission (ACC) and the Bangladesh Financial Intelligence Unit (BFIU) signed a Memorandum of Understanding (MoU) on 4 May 2014 to enhance the opportunity of cooperation to tackle money laundering and other financial delinquencies.
Risk-Based Approach	In January 2015, BFIU released a guideline entitled "ML and TF Banking Sector Risk Assessment Guidelines" (Circular Letter No. 01/2015) to provide fundamental concepts for defining, evaluating and reducing ML & TF hazards. Banks were advised to consider their clients, goods, distribution networks, and geographical places to evaluate their ML & TF risk. They were also advised to evaluate environmental risk, i.e. risks resulting from failure to comply with AML & CFT policies. In compliance with the instruction, all banks have presented their ML & TF risk evaluation reports to BFIU.
Memorandum of Understanding (MOU) BFIU and Other FIUs	BFIU has signed a Memorandum of Understanding (MOU) with other FIUs to improve collaboration with foreign counterparts. To date, BFIU has signed MOU 60 (to date) to exchange ML & TF data with other countries' FIU.

8. Findings and Analysis

8.1 Major Scams and Embezzlement in Banks

The banking industry in Bangladesh is at the risk of cyber-attack and many questions were raised about preventive measures of banks. A study of Bangladesh Institute of Bank Management shows that 43% incidents happened through ATM card, 25% through mobile banking, 15% through ACPS and EFTN, 12% through internet banking, 3% in application software and 2% in other ways. So, the major embezzlement and cyber-attacks for the last few years in Bangladeshi banks are highlighted here.

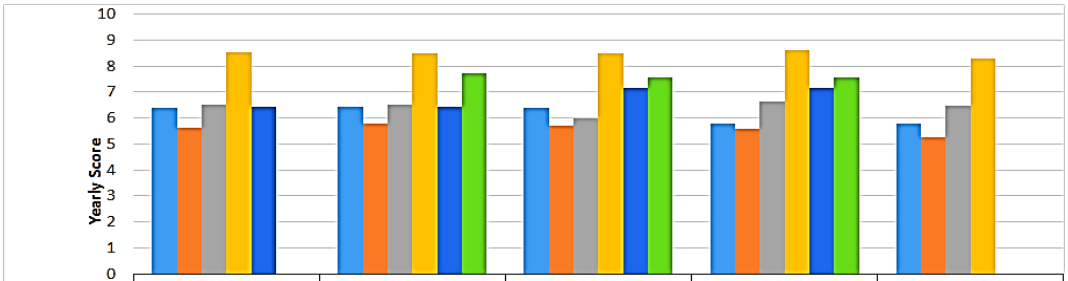
Table 2. Major scams, irregularities and heists in Banks of Bangladesh

Bank/ Institution Involved	Scam	Measures
Sonali, Janata, NCC, Mercantile and Dhaka Bank (2008 -2011)	A bank loan of BDT 4.89 crores with fake land documents. (Dhaka Tribune, 28th August 2013)	The ACC submitted cases against Sonali Bank, Fahim Attire Limited and some people on 1 August 2013; returned to Sonali Bank after the inquiry BDT 1 crore (making the complete BDT 4.89 from the original 5.89 crores). (Dhaka Tribune, August 2, 2013; New Age, August 2, 2013; Daily Star, August 2, 2013)
BASIC Bank (2009-2013)	Misappropriation of BDT 4,500 crores through forged companies and doubtful accounts. (The Daily Star, 28th June 2013)	The ACC lodged 56 cases in September 2015 against 120 individuals charged with swindling. (Bangladesh New Age, 13 August 2018)
Sonali Bank (2010-2012)	Hall Mark and some other businesses stolen BDT 3,547 crores. (The Daily Star, 14th August 2012)	The ACC lodged 11 cases against 27 individuals in October 2012, including the Chairman of the Hallmark Group and the 20 former and present representatives of Sonali Bank. (Tribune Dhaka, 11 July 2018)
Janata Bank (2010-2015 & 2013 to present)	Deceit by Crescent and AnonTex involving BDT 10,000 crores. (Dhaka Tribune, 3rd November 2018)	A panel of investigation, headed by a BB Executive Director, presented a report on the scam to the BB on 30 October 2018. (Tribune Dhaka, 3 November 2018)
Janata Bank, Prime Bank, Jamuna Bank, Shahjalal Islami Bank Ltd and Premier Bank (June 2011-July 2012)	Concealing of BDT 1,174.46 by Bismillah Group and its fake sister concerns. (The Daily Star, 7th October2016)	The ACC lodged 12 cases over the scam on November 3, 2013, against 54 individuals. (The Independent, September 11, 2018)
AB Bank (2013-2014)	Cash laundering of BDT 165 Crores. (The Daily Star,12th June 2018)	The ACC lodged a lawsuit against the former president and representatives of AB Bank on January 25, 2018. (Daily Star, March 12, 2018)
NRB Commercial Bank (2013-2016)	Gross anomalies over distributing loans of BDT 701 crores. (New Age Bangladesh, 10th December 2017)	The central bank assigned an observer to restore discipline and corporate governance at the bank on December 29, 2016. (Tribune Dhaka, 7 December 2017)
Janata Bank (2013-16)	Loan scam involving BDT 1,230 crores (The New Nation, 22nd October 2018)	Thermax demanded that the entire loan be rescheduled again in October 2018 (earlier restructured in 2015). The board of Janata Bank-supported Thermax's suggestion and sent it for approval to the BB. (Daily Star, October 21, 2018)
Farmers Bank (2013-2017)	Fund theft of by 11 companies e.g.: NAR Sweaters Ltd, Advanced Development Technologies, etc. involving BDT 500 crores. (The Daily Star, 24th March 2018)	In January 2018, the BB directed Farmers Bank to perform a functional audit on loan accounts in its Motijheel branch with an exceptional sum of at least BDT 1 crore. (Daily Star, 24 March 2018) In April 2018, four suspects were detained by the Anti-Corruption Commission (ACC), including the former Chairman of the Audit Committee of the Farmers Bank. (The Independent, April 11, 2018)
Bangladesh Bank (February 5, 2016)	The heist of BDT 679.6 crores (USD 81 million) by international cyber hackers from reserves account of Bangladesh Bank with the New York's US Federal Reserve Bank. (The Daily Star, 5th August 2017)	The government created a 3-member inquiry committee on March 19, 2016, led by former Central Bank governor Dr. Farashuddin. (Daily Star, August 5, 2017)
Dutch Bangla Bank Limited (May-June, 2019)	Tk 16 lakh stolen by the members of the international hacker group. They used Tyupkin Malware to make the ATM infected and to stop all network connections and there is no record of the transactions. (The Daily Star, June 11, 2019)	Six Ukrainians were detained on 1 June 2019. This problem is being investigated jointly by the Detective Branch, Counter-Terrorism and Transnational Crime Cybercrime Unit (CTTC) and CID.

Note. Report on Banking Sector in Bangladesh, Centre for Policy Dialogue, 2018.

8.2 Comparative Trend Analysis of the Basel AML Index of South Asian Countries

The Basel AML Index indicates the overall score calculated as the weighted average of 14 signs dealing with AML/CFT regulations, exploitation, financial standards, political revelation and the rule of law are combined into one overall risk score. The Basel institute depends on data from openly accessible sources such as FATF, Transparency International, The World Bank, and The World Economic Forum. It shows the vulnerability of a nation in such a way instead of evaluating the measure of unlawful cash or exchange.



	2014	2015	2016	2017	2018
Bangladesh	6.38	6.43	6.4	5.79	5.78
India	5.64	5.77	5.69	5.58	5.28
Pakistan	6.53	6.52	6	6.64	6.49
Afganistan	8.53	8.48	8.51	8.6	8.28
Sri Lanka	6.42	6.44	7.16	7.15	0
Nepal	0	7.71	7.57	7.57	0

Figure 1. Comparative trend analysis of the Basel AML index of South Asian Countries

Source: Basel Institution on Governance, 0= low risk, 10=high risk.

***** Bhutan and Maldives not included in the index.

From the Fig.1. We found that Bangladesh has been put fifth before India among the six South Asian Countries since most recent five years as per AML List. Basel AML Index, 2018 was based on the overview of 129 countries according to their risk of ML and TF. In 2018, the score of Bangladesh was 5.78 (51st position) followed by India (68th position). Afganistan is holding most astounding score with high hazard position since its incorporation in the Basel AML record. On the other hand, India is holding the lowest score in the last five years among the six above stated South Asian Countries. The score of Bangladesh is gradually decreasing in 2017 and 2018 compare to 2016.

9. Potential Banking Systems Intrusions

9.1 Distributed Denial-of-Service Attack

Disavowal of Service (DoS) is placed after psychological warfare and secret operations as the third most notable risk of the FBI. Budgetary organisations facing DoS attack could face amazing money loss owing to customer and customer loss. It is also a mind-boggling cost needed to solve the attack harm. The most commonly acknowledged attack that could happen in the financial framework is Conveyed Denial of Service (CDoS). CDoS includes at least hundreds of zombie PCs to deliver the attack to the framework-focused. Before an attack occurs, the assailant manufactures an organized attack by examining an open port, inadequately secure PC with no firewall or programming hostile to infection. In the 'zombie' PC, another program is implemented. The program can self-proliferate and therefore create an enormous arrangement for attack. It may comprise both the code for a variety of attacks and some vital framework for remote control interchanges. These' zombies' would meanwhile send an enormous amount of packages to the frame and power the real parcels mentioned to fall due to a break. This kind of interruption can influence the accessibility and coherence of the financial framework. The monetary organization would neglect to direct exchange with its client, colleague, and sellers.

9.2 Data Breach

Monetary establishments need to mindful about dangers that would influence the framework security in their association. An information break, one of the risks exists enables the data and information to go out from the framework, making it visible to other people. An information break is a very notable wonder where it includes exceptionally delicate and secret information that may have been seen, stolen, and furthermore have been utilized by any individual or any association without being approved to do as such. For instance in security information break, a situation where includes five Connecticut banks are coming about because of security

information rupture, influenced by New Jersey an organization that procedures MasterCard installment, as per the paper and web reports. The impact of the information break takes on an extraordinary number of misfortunes for the money-related organization where, for example, their Visa organizations, Visa and MasterCard, reached them about the break, as indicated by the BankinfoSecurity.com web page. The banks that influenced the rupture are Litchfield Bancorp, Cheshire's Apple Valley Bank, Norwich's Dime Bank, Middletown's Liberty Bank, Chelsea Groton Bank, and 230 other budget foundations.

9.3 Malware

Malware is a programming program that intends to modify and alter the PC's structure without the expert client or owner, and this malware moves from PC to PC and organizes scheme. Malware may include infections, Trojan ponies, worms, content assaults, and maverick web code. Malware attack can impact the privacy, sincerity and availability of the financial framework. Malware attacks in privacy typically include catching keystroke numbers, passwords, and MasterCard numbers, transferring and downloading documents, and seeing what's going on the server screen. An assault against honesty anyway is likewise hurting the financial framework, where it changes the framework, for example, the contaminated record and furthermore information. The defilement of information records and furthermore application documents by unapproved document scholars, changing designs of the financial framework and furthermore overwriting information are all impact the trustworthiness of the financial framework. The accessibility of the financial framework may also be influenced by the erasure of records and sub directories, the renaming of papers, the rebooting or weakening of safety frameworks and the forswearing of administrative attacks.

9.4 TCP/IP Spoofing

One of the basic types of the Internet coverage is TCP / IP satirizing. In IP caricaturing, an aggressor improves unauthorized access to a PC or system by causing it to give the impression that the machine's IP address has originated from a vindictive message entrusted to the machine by "parody." IP address parodying is the technique by which the assailant can send bundles on a scheme without the firewall structure being caught and obstructed. For most of the channel, these firewall frameworks were any external IP address that tried to talk to it. Notwithstanding, utilizing IP caricaturing, the aggressor can veil its personality by making their IP address to seem to originate from the interior system, in this manner making the firewall unfit to capture it, thus parcels can undoubtedly move by the assailants. The goal and objective for this assault is to empower the assailant to pick up root access to the injured individual server, for this situation the financial framework, permitting the formation of an indirect access section way into the focused on frameworks. Wherever the escape clause is guaranteed for the previous attack, there is a secondary passage for the aggressors to sneak back to the server whenever necessary.

10. Cyber Payment Frameworks and Possible Misuse of Them for Money Laundering

As a tool, the exchange of important electronically valuable cyber payment systems takes place. Such exchange occurs through the use of the internet as a medium or through the use of a valuable sorting card. Cyber payment systems are meant to replace some retail and buyer-level exchanges with cash. Cyber payment systems also pose fresh challenges for law enforcement agencies. With the help of present-day innovation, these frameworks can consolidate the highlights, e.g. present bank-based wire move speeds and money-namelessness together. Such problems should be discussed as the goal for improving such frameworks is to ensure recognition and anticipation against illegal tax avoidance and associated illegal exchanges. Basically, we can say that cyber payment systems talk to the outcomes of the convergence between the progressive disturbances in information technology and strong trends to market de-guidelines that occur in the electronic business world as shown in figure 2.

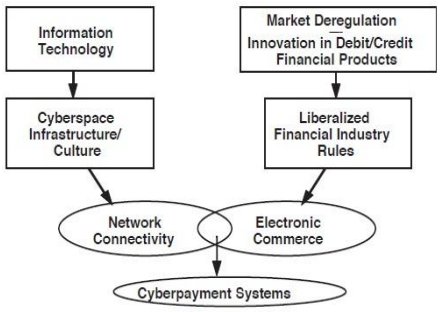


Figure 2. Cyber payment systems and payment system dynamics

10.1 Investigative Techniques on Cyber-Payment to Identify Potential Cyber Laundering

Two changing features create possibilities in cyber payment systems for remote interrogation of transaction documents. First: The generation of tags during the transfer of value, meaning that the funds shifted from one cyber deposit to another instrument, revealed transaction data with unique markers. The second feature is the integration in cyber payment networks with the open network standards featured in the TCP / IP internet protocol suite. The IP (Internet Protocol) "tunneling method" would allow the segregation of "value transfers" from other internet traffic to ensure the integrity of their customer connections and make it easy for government authorities to track suspicious flows of drug trafficking and money laundering funds. It is a daunting mission for the authorities to carry out any kind of surveillance of information flows over the internet due to the enormous quantity of network traffic. Strict Web service customers involved in e-mail and e-commerce privacy policies also limit the acceptability of network message content requests. Keeping in mind Internet privacy policies, law enforcement apps are difficult to approve sensitive data records, but there is a greater possibility that network traffic will be more acceptable to affect client organizations if it can be categorized or differentiated by the nature of the information being transmitted. Differentiating information itself raises questions about how to filter unstructured network information and enable the capture of distinct data kinds and other data for safe transmission. Data differentiation itself raises questions as to how unstructured network information should be filtered and enables distinct data types and other information to be captured for secure transmission. These two points help to set up network audit and traffic analysis tools to evaluate the amount and nature of information flow. The initiation and termination points in IP Tunnels are, as shown in Figure 3, IP addresses. Since many networks allocate these addresses dynamically (for customers to allocate network connections through available addresses), the available subset of IP addresses should be set aside for value transfers alone.

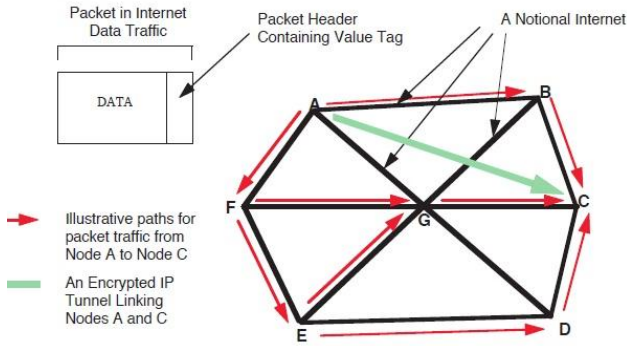


Figure 3. IP tunneling application concept for cyber payment systems

A tag placed on a message of value transfer would invoke a distinctive protocol (called the Cyber Security Protocol-CSP) in TCP / IP, generating a virtual (and encrypted) connection between two known IP addresses. The constructed IP tunnel would therefore, work as the conduit where the value transfers could be performed. "Servers would require CSP-related network traffic logs to be maintained using TCP / IP with built-in CSP features. Such documents would then be created accessible for judicial review by law enforcement and payment agencies". The alternative to this requirement would be to generate "CSP Traffic Reports" through the network operating system through an autonomous smart agent application. This application could record importance by placing servers close to CSP-designated IP addresses and transfers and returning information to secure servers maintained for cyber payment by the supervisory authorities.

10.2 Positive & Negative Cyber-Related Payment Factors

In the perspective of the authors, the following benefits (favorable) and negative factors are linked to cyber-based payments after analysis of various types of literature:

Positive Factors	Negative Factors
o Easy operation of the company. o Low-cost operations increase business. o Provide a number of payment techniques. o E-money value transfer minimizes the burden of carrying enormous traditional money. o Easy to pay within the boundaries of authority. For instance, payment of credit/debit cards issued by SEB / Swed bank in another region such as Asia. o Provides the facility for direct transactions between two parties without involving a third party. o It improves the confidence of the company community. o Theft financial safety (bank cards or other intelligent cards). Can be canceled or blocked by Phone / Email if lost or misused. o Giving an enormous boost to worldwide e-commerce companies. E-Bay, Amazon, and Alibaba (Ali express) and many more online retailers are the current real-life examples. o The cyber-payment scheme offers interconnections between various economic institutions that assist to keep the economic momentum.	o Identity theft (Cyber Payment Products) related to bank / financial customers. By adopting various techniques such as hacking, using fake ids, etc., cyber launderers can take advantage of the cyber payment system for cyber laundering. o Costly keeping up-to-date (with the recent associated techniques) and maintaining Cyber payment systems ' big facilities. o Because of privacy concerns, banks are unwilling to provide law enforcement agencies with data about their clients that may be harmful to society. o Millions of transactions performed every day is difficult to track or investigate unless a specific transaction is discovered to be very suspicious. o Possibility of misuse by criminals of cyber-payment goods such as debit/credit cards for internet payments from stealing data collected from countless internet websites or other sources such as hacking. In the western world, such events are very prevalent. o No restrictions that only the owner of the bank card / payment (Cyber Payment Products) can withdraw or deposit cash in ATM or pay online. This encourages criminals to take advantage of their financial benefits.

11. Recommendations

- Ensuring good supremacy in the tax administration to uproot money laundering.
- Customs authority needs to be watchful in screening both import and export shipments to scrutinize the quantities revealed in their Letter of Credits.
- The government should give exemplary punishment to those who are linked with cyber laundering to save the country from huge economic loss.
- An organized audit of customs and banks to prevent trade-based laundering.
- Assuring a safe environment for investment locally and to prevent capital flight.
- To avoid online banking frauds banks should emphasize the training of employees regarding Cybersecurity systems.
- Multi-factor verification method should be applied.
- Continuous research and development to develop a new security system for banks.
- To develop IT infrastructure and IT governance.
- Create responsiveness among customers and management of banks.
- To take state-sponsored Cybersecurity initiatives and budget allocation.
- Co-ordination and unceasing follow-up is needed to make progress in bringing back laundered money by the professional bodies.

12. Conclusion

Cyber laundering is a sparingly significant crime. The estimated cash laundered worldwide each year, according to UNODC, in the present US dollar is $800 billion to $2 trillion. The “Dirty Money” enters the global banking system and its source is hard to define. Cyber laundering debases the financial market and confounds the public trust in the global financial system. A correct measure of cyber laundering may help to mitigate more accurately the offences, the clandestine nature of illegal conduct supported by criminals. Indeed, the traditional system to prevent laundering is no longer works. The banking industry in Bangladesh is experiencing ATM fraud, trade-based concealing, website hacking, credit card fraud, etc. The deep-rooted offenders have linkages with political leaders, bankers, officers and provide cover for prearranged crimes. It is high time to make a trade-off between the precautionary framework and to employ effective Cybersecurity system. The government should

re-design the anti-money laundering initiatives and monitor cross-border transaction payments. A large amount of money should be invested in IT infrastructure in banks. There must be a linkage between banks and government law prosecution agencies. The banking authority should monitor and report to the concerned authority about any suspicious transactions. Establishment of good corporate governance and effective legal framework may help to combat cyber laundering activities. Further research could focus on developing a theory or techniques to detect and fight against cyber laundering.

References

Akin, O. (2016). Effects of Money Laundering on the Economy of Nigeria. *Beijing Law Review, 7*(2), 158-169. https://doi.org/10.4236/blr.2016.72017

AnandTech Forums: Technology, Hardware, Software, and Deals. (2008). *World Bank under Cyber siege in Unprecedented Crisis*. Retrieved August 10, 2019, from https://forums.anandtech.com/threads/world-bank-under-cybersiege-in-unprecedented-crisis.226073

Bangladesh Customs Gov. (2012). *Money Laundering Prevention Act, 2012, the Peoples of Republic of the Government of Bangladesh*. Retrieved from http://www.bangladeshcustoms.gov.bd/download/Money_Laundring_Prevention_Act_2012-English_Version.pdf

Basel AML Index. (2018). *The Basel Institute on Governance (2014-2018)*. Retrieved from https://www.baselgovernance.org/elearning-and-tools/basel-aml-index

Centre for Policy Dialogue (CPD). (2018). *Banking Sector in Bangladesh: Moving from Diagnosis to Action*. Retrieved from https://cpd.org.bd/wp-content/uploads/2018/12/Banking-Sector-in-Bangladesh-Moving-from-Diagnosis-to-Action.pdf

Dhaka Tribune. (2017). *4 Ways money is laundered out of the country.* Retrieved from https://www.dhakatribune.com/business/economy/2017/06/18/4-ways-money-laundered-country

Dhaka Tribune. (2018). *Majority of banks still vulnerable to cyber-attacks*. Retrieved from https://www.dhakatribune.com/opinion/special/2018/02/05/majority-banks-still-vulnerable-cyber-attacks

Editorial Team. (2000). *Full Text of OCC Guidance to Bankers and Examiners on Infrastructure Threats and Intrusion Risks.* Retrieved August 10, 2019, from https://www.americanbanker.com/news/full-text-of-occ-guidance-to-bankers-and-examiners-on-infrastructure-threats-and-intrusion-risks

Forbes.com. (2019). *How to Hack a Bank*. Retrieved from https://www.forbes.com/asap/2000/0403/056_3.html

Guidelines for prevention of ML & TF. 2019 circulated by Anti Money Laundering & Combating Financing of Terrorism Division, the Peoples of Republic of the Government of Bangladesh.

Ikhtiar, M. (2017). *Money Laundering in Bangladesh- Causes, consequences and remedies*. Retrieved from http://www.newagebd.net/article/28777/causes-consequences-and-remedies

Information Security magazine Readers. (2009). *2009 Information Security magazine Readers' Choice Awards - Information Security Magazine.* Retrieved August 10, 2019, from https://searchsecurity.techtarget.com/magazineContent/2009-Information-Security-magazine-Readers-Choice-Award

Institute for Defence Studies and Analyses. (2016). *Bangladesh Bank: The Billion Dollar Breach*. Retrieved from https://idsa.in/idsacomments/bangladesh-bank_the-billion-dollar-breach_msharma_230316

Md. Joynul, A. (2018). *Money Laundering: The Dark Secrets*. Retrieved from https://www.daily-sun.com/printversion/details/319989/2018/07/06/Money-Laundering:The-Dark-Secrets-

Md. Solamain, S. (2019). *62 pc banks are at risk of cyber-attacks.* Retrieved from https://www.daily-sun.com/printversion/details/381059/62pc-banks-at-risk-of-cyber-attacks

Mike, M. (2009). *Bank Sends Confidential Email To Wrong Address, Hauls Google To Court To Figure Out Who Got The Email*. Retrieved August 10, 2019, from https://www.techdirt.com/articles/20090922/0440136280.shtml

Molander, R., Mussington, D., & Wilson, P. (n. d.). *Cyberpayments and Money Laundering Problems and Promise Critical Technology Institute.* Retrieved from

https://www.rand.org/content/dam/rand/pubs/monograph_reports/1998/MR965.pdf.

Moore, D., Shannon, C., Brown, D. J., Voelker, G. M., & Savage, S. (2006). Inferring Internet denial-of-service activity. *ACM Transactions on Computer Systems*, *24*(2), 115-139. https://doi.org/10.1145/1132026.1132027.

Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector.* Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14420.pdf

Ricky, L.(2018). *Cyber Security Regulations in the Banking Sector: Global Emerging Themes*. The London School of Economics and Political Science.

Roger A. G. (2001). *Malicious Mobile Code: Virus Protection for Windows*. Retrieved August 10, 2019, from https://www.amazon.com/Malicious-Mobile-Code-Protection-Windows/dp/156592682X

Saiful, Akter, & Zahed. (2017). Predicate Offences of Money Laundering and Anti Money Laundering Practices in Bangladesh among South Asian Countries. *Studies in Business and Economics*, *12*(3). https://doi.org/10.1515/sbe-2017-0037

Shamsus, S. (2016). Effect of E-Banking on Banking Sector of Bangladesh. *International Journal of Economics, Finance and Management Sciences, 4*(3), 93. https://doi.org/10.11648/j.ijefm.20160403.11

Sultana, S. K. (2016). Cyber Crime scenario in the banking sector of Bangladesh. *The Cost and Management, 44*(2).

The daily newnation. (2018). *Stopping money laundering.* Retrieved from http://m.thedailynewnation.com/news/179762/stopping-money-laundering (2018).

The Financial Action Task Force. (2013). *Financial Action Task Force: Annual Report, 2012-2013*. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF%20Annual%20Report%202012%202013.pdf

The financial express. (2018). *Checking money laundering*. Retrieved from http://www.thefinancialexpress.com.bd/views/views/checking-money-laundering-1533395518

The financial express. (2018). *Money laundering and NPL interlinked*. Retrieved from https://thefinancialexpress.com.bd/economy/bangladesh/money-laundering-npl-interlinked-1553139964

Thedailystar.net. (2018). *The hidden dangers of money laundering*. Retrieved from https://www.thedailystar.net/opinion/the-overton-window/the-hidden-dangers-money-laundering-1569517

United Nations Office on Drugs and Crime. (n. d.). *Money Laundering and Globalization*. https://doi.org/10.1111/j.1467-6478.2008.00446.x

Zali, M., & Maulidi, A. (2018). Fighting Against Money Laundering (December 5, 2018). *Brics Law Journal*, *V*(3). https://doi.org/10.2139/ssrn.3296154