Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

COUNTERMEASURES AGAINST INTERNET-BASED MONEY LAUNDERING: A CONCEPTUAL STUDY

LEELIEN KEN HUANG
FENG CHIA UNIVERSITY
Leelien.huang@gmail.com

ABSTRACT

In 2012, the number of the Internet user has reached 7 billion globally according to Internet World Stats. Among of all Internet users, approximately 50% of them are predicted to be on line shoppers in banking, investment and retailing services. As a result, it is reasonable to assume that the greater the level of the Internet usage, the higher is the risk of money laundering through the Internet. Bank operations manager and law enforcements were interviewed. Based on the findings, we propose a three-stage conceptual framework of countermeasures against Internet-based money laundering. Practitioners may refer to this as guidance for anti-money laundering policy while dealing with Internet-based money laundering issues. Implications are discussed.

Keywords: Internet, Countermeasures, Internet-based Money Laundering

INTRODUCTION

To disguise or conceal large illegally obtained gains generated from crime is a physical effort spent since criminal activities exist in the country. Legitimate is an incentive to money laundering for organised crime, for example drug trafficking, and acts such as smuggling, illicit weapon sales, embezzlement, ransom, and even computer fraud schemes. The activity of money laundering is usually a cross boarder issue that involves bank secrecy to protect financial records, government's attitude to counter money laundering, whether or not SWIFT member, and corruption. Any of those indicators would determine the extent of two basic elements of conducting money laundering: convenience and less-attention from law enforcement authority, which are various, from one jurisdiction to another.

By nature, money laundering occurs in black market where not inside of normal economic activity and statistics is [14]. A large scale of money laundering would produce the adverse macro-economic effects on changes in money demand; interest rate and exchange rate volatility; tax collection and fiscal policy. For the private sector, money laundering may reduce the cost of capital for illegal organization and provide a competitive advantage over legal business entity. For the banking sector, money launderers commonly use financial institutions as intermediaries to process funds derived from criminal activities. If these illicit funds can be easily processed through a particular bank that may be unwittingly used or not, risks to bank asset quality would be heightened. From social and political point of view, if anti-money laundering system is ineffective, organised crime may infiltrate financial institutions and control major sector of economy by investment. These organised criminal activities may cause social ethical standards distorted and government democratic transition obstructed.

Thus, in respond to national and inter-national money laundering concern, in 1989, G7 established the Financial Action Task Force (FATF) in Paris to coordinate money laundering issues by setting standards such as

Forty Recommendations to counter money laundering and terrorist financing [7]. Member of the FATF currently has 31 countries and governments and two international organizations; and more than 20 observers. Many non-FATF member countries have recognized Forty Recommendations as international standard for anti-money laundering and initiate their own countermeasures [7].

As international co-operation in anti-money laundering grows substantially, however, money launderers keep looking for new more sophisticated money laundering routes to avoid investigation from law enforcement agencies. In past years, the rapid explosion of the Internet may provide money launderers access to and from a foreign bank in any jurisdiction where has less stringent anti-money laundering law and help hide their identity in network laundering process. Conventionally, legitimizing illegal profits is usually limited to physical cash purchase of real property and personal valuables, or scurry of cash deposit into account through financial system with direct or indirect contact. At present, the arrival of electronic payment with security and privacy through computer network may attract money launderers. Despite no available concrete indicators for such use by money launderers and various trends for Internet-based laundering geographically, the potential negative impact cannot be neglected by legislative authorities, law enforcement agencies, and banking supervisors.

This paper does not attempt to examine statistical significance of countermeasures against money laundering, but attempt to propose conceptualized countermeasures that expect to be guidance for law enforcement authorities, national legislators, and international organizations to achieve agreement on seeking to appropriate amendments to countermeasures. The remainder of our study proceeds as follows. First, the concept of money laundering is presented. This is followed by both money laundering scheme of the Internet and issues on the Internet-based laundering. Next, the methodology is provided. Based on findings, we then provide implications of concepts of countermeasures against Internet-based laundering. Lastly, conclusions and limitation are presented.

CONCEPT OF MONEY LAUNDERING

Money laundering refers to the process of concealing illicit gains generated from criminal activity [8]. By successfully laundering the proceeds of a corruption offence, the illicit gains may be enjoyed without fear of being confiscated [8]. In a sense, money laundering is the approach of hiding the illicit source or illicit application of income, and then transforming that income to be legitimate [18]. Conventionally, physical cash payment is the most popular means of money laundering. The key point of laundering process is to avoid unwanted attention from legal enforcement agencies. According to Intriago [9], followings present three basic phases of money laundering.

In the beginning placement phase, the launderers deposit their illegal activity proceeds into the financial system. In order to avoid detection, the large sum of tainted proceeds might be divided into less conspicuous smaller amounts that fall beneath bank regulatory reporting limit (e.g., USD 10,000 in the US, and USD 50,000 in Taiwan) and then deposited into bank accounts or subscribed a series of financial instruments under disguised beneficiary. However, the structure of this initial stage is usually fragile and easily leaves traceable records. Thus, the laundering process would deepen into the second phase: layering.

When entering layering phase, the launderers might try to generate indistinct existence of illegal profits by a series of complicated bank transactions or movements of the funds to be distant from illegal origin. The layering approach might be continuous purchases and sells of financial instruments and directly wire laundered proceeds into foreign banks in jurisdictions with lax record keeping and reporting requirements. The structure of the second phase is more solid and leaves blurred and distant trail records. Finally, in the integration phase, the launderers put these funds in circulation into a normal economy system through legal spending on luxury goods, contracting on service, investment on real estate or financial assets, and even lending in the form of legitimate money.

As such three phases, in Figure 1, money launderers tend to seek for foreign countries or territories where there is ineffective counter money laundering law and return illicit funds to original individual at ultimate destination. During the initial laundering, in the country where illicit funds generated, it is seen that banking systems are mostly used to transfer funds that are often processed through underlying activities with directly depositing cash into bank accounts or smuggling cash to laxly regulated jurisdictions where money launderers base their operations. When the launderers move the illicit funds into a less anti-money laundering control area, they may choose an offshore bank offering adequate financial infrastructures and transit bank accounts through withdrawing cash, purchasing negotiable certificates (e.g., travel's check, NCD, international money order, bond and stock), or wiring at various locations to make transactions complicated and difficult to trace.

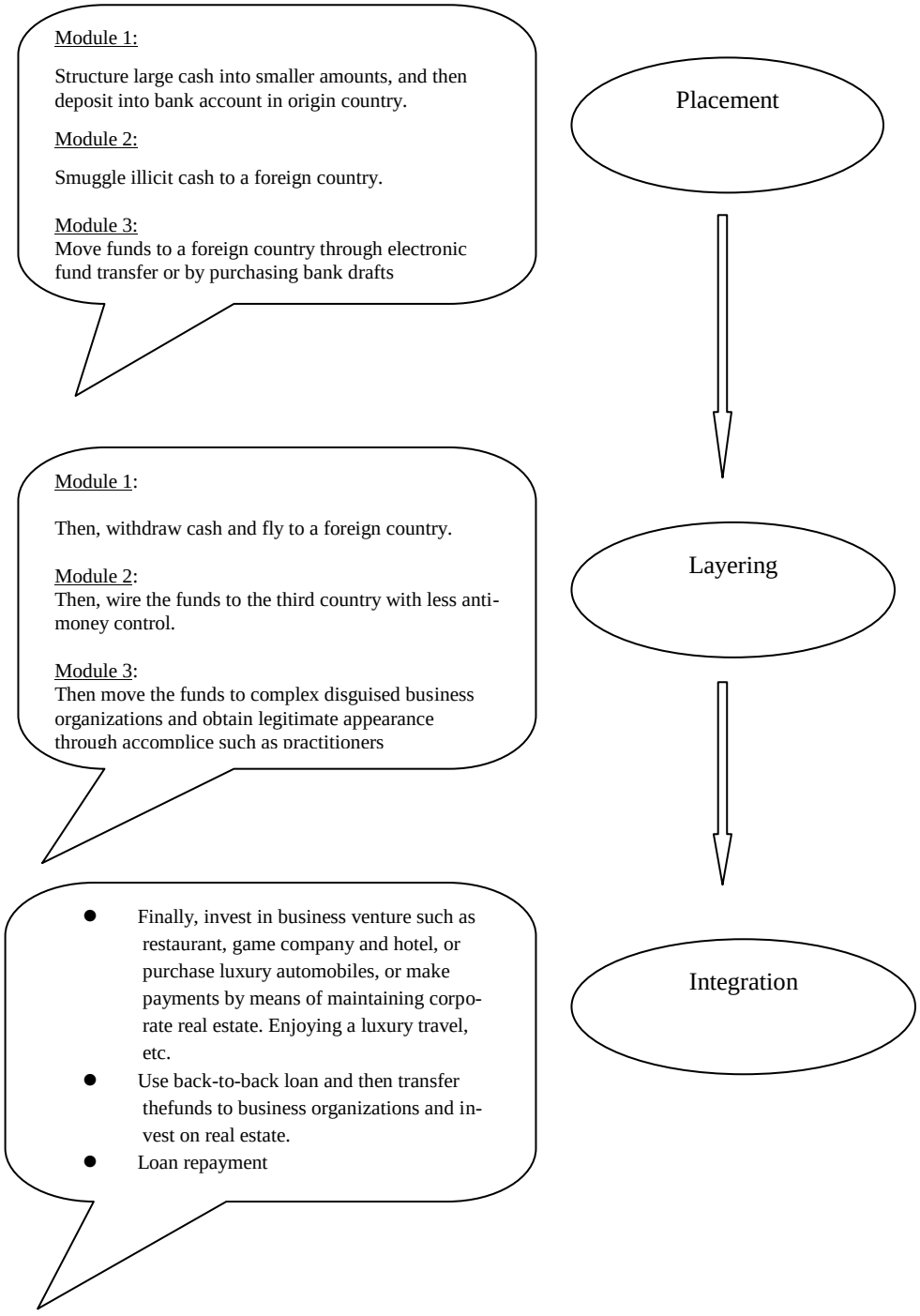

Figure 1: Selected Typical Module for Classic Money Laundering

At the stage of layering, this process can be done without leaving traces of sources and transfer the seemingly legitimate funds to final destinations: laundering paradise or origin country. To enjoy illegal profits safely is the purpose of money laundering. At the stage of integration, the launderers would purchase luxury items, financial valuables, sell real estate or place investments on private businesses to control main sectors of normal economy. In addition to those, the launderers might finance a front company by lending technique to conceal illicit funds and then enjoy tax deduction from interest payment. The modules shown in Figure 1 should not be regarded as the only optimal techniques of money laundering. As anti-money laundering law reinforced and international fight against money laundering more emphasized, the tendency to use the Internet based transaction to avoid detection gains attention recently.

INTERNET-BASED MONEY LAUNDERING

As stated, convenience and anonymity are attractiveness to the launderers. Internet access has these features. The probability of using the Internet as a laundering channel could be high since the Internet has grown dramatically from its inception in the late 1970s to today's truly global medium. For example, more than 2.8 billion people in the World have Internet access in 2013 [10].

Through the Internet, the launderers take advantage of quickly transacting the illicit funds without extra supporting technology. Simultaneously, a variety of secure electronic payment systems such as electronic fund transfer and debit card (e.g., ATM card), stored value card (e.g., Mondex and VisaCash), credit card based payment (e.g., Ecash and Echeck) were being developed to protect confidentiality and authentication. At present most companies use SSL (Secure Socket Layer) protocol to provide security and privacy. More secured protocol, called SET (Secure Electronic Transaction), was developed jointly by Visa and MasterCard in 1997. This protocol provides more complex security scheme that applies encryption, digital signature and message digest. It also requires certificates and certifying authorities.

Although these improvements on security and privacy can be considered as positive contributions to efficient customer transaction and cost reduction for financial systems, they also make financial institutions and/or law enforcement more difficult to examine the launderers' identification and give an appealing opportunity to them. Especially in recent years, mobile banking through smart phone is prevailing with certain Internet wireless technology payments such as NFC (near field communications), SE (secure element), and TSM (trust service managers). Because mobile devices have a smaller form factor and therefore are more susceptible to loss or theft. This is pretty easy for the launderers disguise their identity using stolen mobile devices protected by payment security systems [13]. As such, cashless payment and remote laundering through the Internet will come to be the new type of detergent that allows for cleaning dirty money.

Nevertheless, the idea of money laundering electronically is not a new one. A typical example of cashless payment is electronic fund transfer (EFT) that has been mostly used to possess a nearly risk free conduit for moving money between countries. For example, in the United States, there are three major electronic fund transfer systems: SWIFT (Society for Worldwide Interbank Financial Telecommunication), CHIP (Clearing House Interbank Payment System), and Fed-wire that is something like that called IBRS (Inter-Bank Remittance System) in Taiwan. However, this illicit fund transfer with limited information regarding the party involved can be easily hidden because of large wire transactions occurring daily. More explicitly, Table 1 shows non-cash payments that may be preferred by the launderers.

In Table 1, basically, the launderers would employ electronic cashless payments as illustrated when conducting money laundering through the Internet. Following the continuous growth of on-line banking facilities providing services such as direct payment, EFT, issue of checks, subscription of bond, security, and mutual fund, credit card cash advance, and open/closing of bank accounts [17]. The launderers can easily open bank account with fake registered identity on any Internet service provider (ISP) located in a remote area and structure the illicit funds into different difficult-to-trace layers without physical presence. When lastly enter into integration, the launderers legitimize the illegal profits by diversifying the payment method into non-cash instruments and by trading goods and services on line. Table 2 indicates selected items mostly purchased on line and probably used by the launderers to make the illicit funds appear legally.

Table 1: Technology-Based Payment Attraction to Money Laundering

Payment Instrument Status	Medium
Credit Card Online	POS (Point of Sale)
Online	EDC (Electronic Data Capture)
Offline	Imprinter
ATM card/ Check Card Online	Auto Teller Machine
Stored Value Card (Smart card) Offline	POS
Paper Check Online	ACH /VAN
EFT Online	CHIPS
Digital Cash Online	

Table 2: Items Purchase Online

Order	Item	Percentage of Responses	Count of Responses
11	Banking	12.1%	78
12	Investment	11.8%	76
16	Autos	4.3%	28
18	Insurance	2.5%	16
20	Real Estate	2.0%	13
21	Jewelry	1.6%	10
	Total	**34.3%**	**221**

** The rest of items are omitted to show in this Table due to low unit price that the launderers might not select to consume their large sum of illicit money. However, it does not mean the launderers would not choose them at all.*

Among those non-cash instruments, credit card is the most popular payment method for cyberspace shopping today. An example of Internet-based money laundering by means of credit card payment is shown in the Figure 2. In this example, the launderers would establish an offshore website company that provides service through the computer network. The launderers then hire couriers under their control to utilize this Internet service charging on credit card or debit card tied to bank account which has the illicit funds deposited. After the service rendered, this offshore website company invoices acquirer bank or the credit card company to claim the payment by capturing process. Then, acquirer bank or the credit card company bills the launderers' bank account through the Internet. Therefore, the launderers can legitimize their criminal proceeds by simply controlling bank account and offshore website company Internet service.

The electronic credit card system on the Internet has a feature that each entity such as ISP, Internet invoice service, certificate authority, and payment gateway including the launderer's bank, acquirer bank or the credit card company can only see the partial information because of secure transaction protocol as above mentioned [6]. Thus, it makes transactions more difficult to trace.

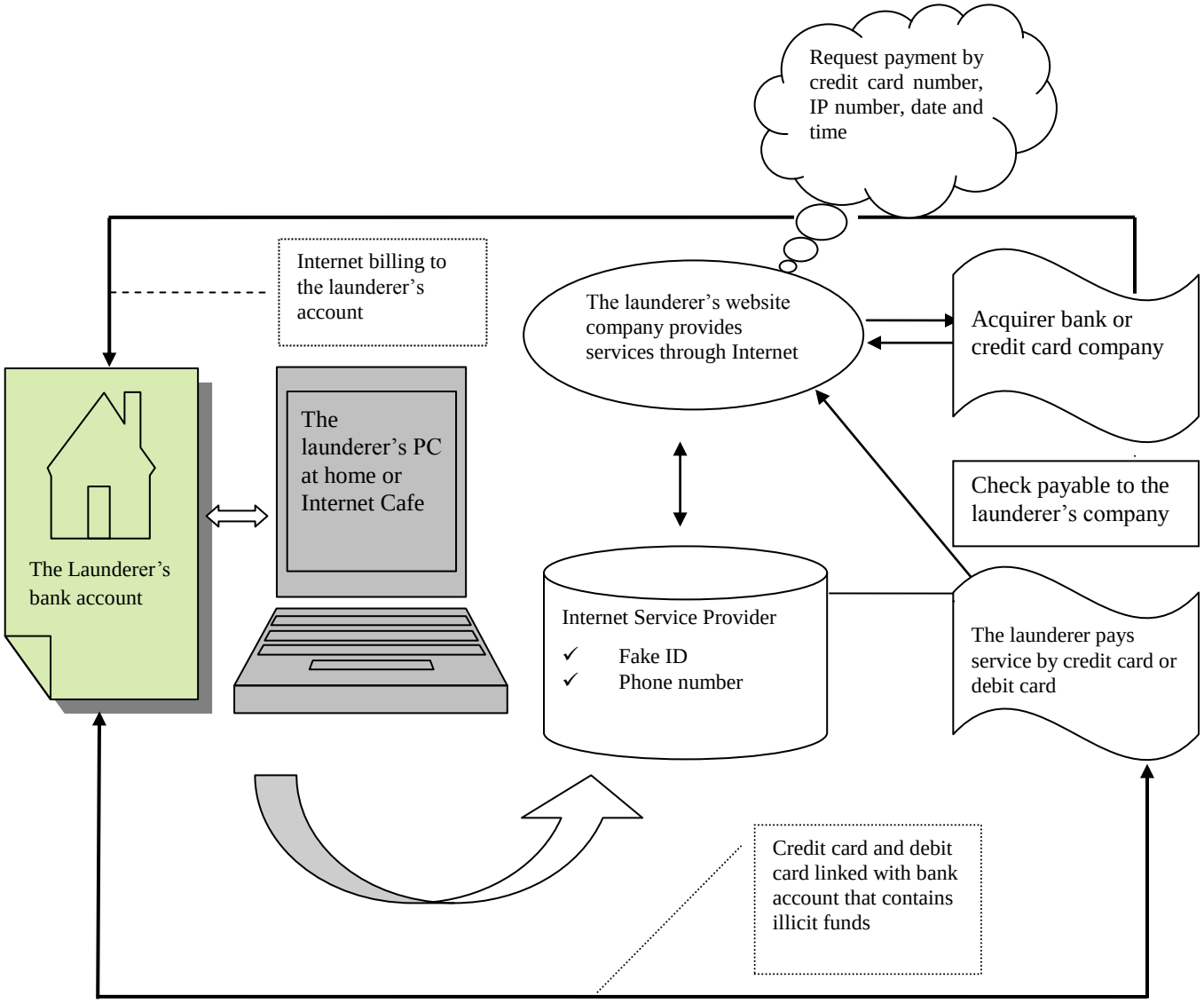

Figure 2: Internet-based Money Laundering by Credit Card Payment

Another example of Internet-based money laundering would be the use of Ecash or digital cash. Ecash was developed by DigiCash (http://www.digicash.com) that is Holland and the United States based company to allow fully anonymous secure electronic cash to be used on the Internet. Ecash is defined as a series of numbers that have an intrinsic value in the form of currency. The security is improved by extensive use of both symmetric and asymmetric cryptography (i.e., digital blind signature techniques) required for open computer network. Ecash worth real monetary value has been available on the Internet through which Mark Twain bank of St. Louis (http://www.marktwain.com) has started issuing Ecash in U.S dollars since 1995. Hence, Ecash may become a particular interest to money launderers and law enforcement authorities because of its unconditionally untraceable trait.

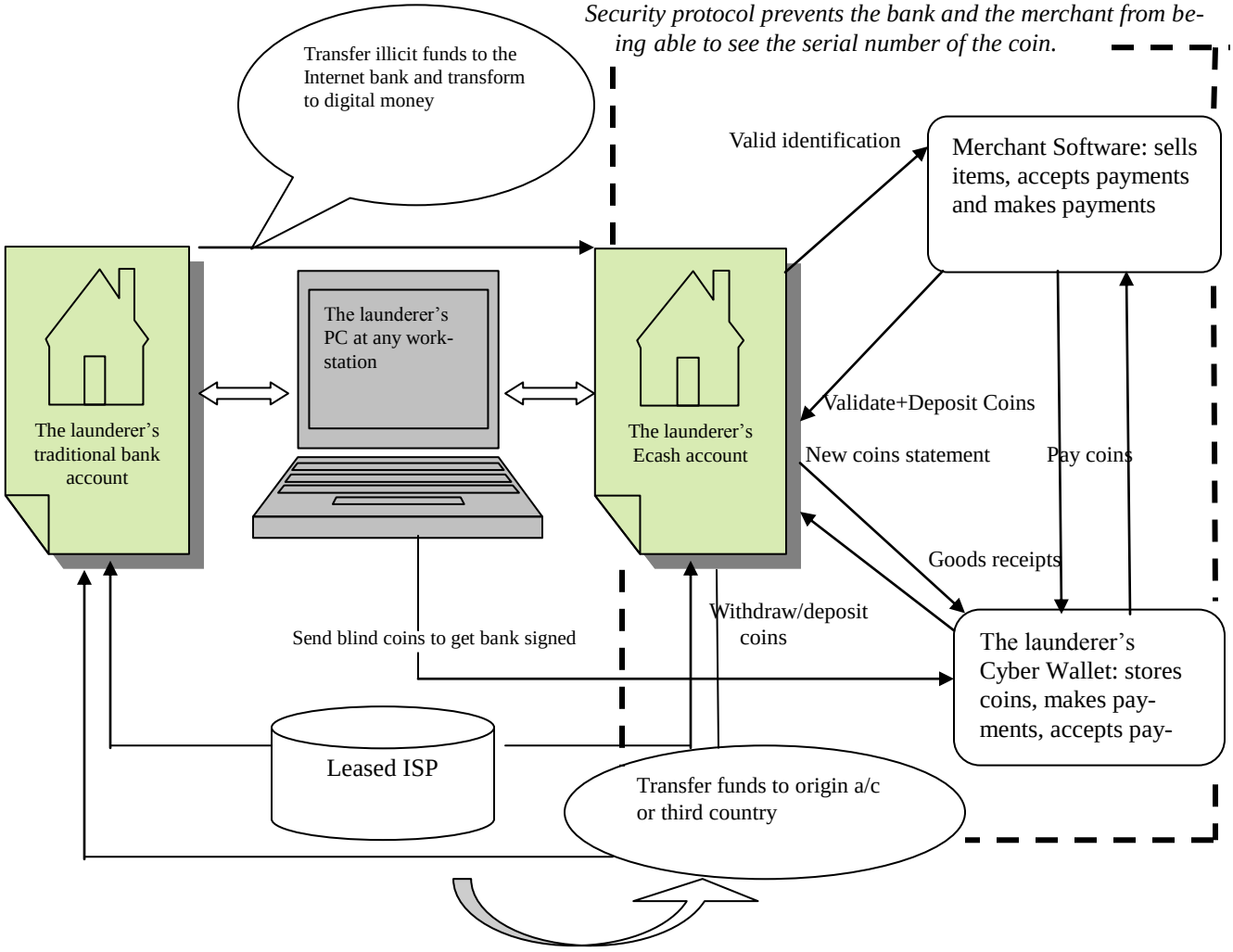

Figure 3: Internet-based Money Laundering by Ecash

In the Ecash laundering module, firstly the launderers have to structure the illicit funds within reporting limits into several traditional bank accounts under different names in different financial institutions. This stage of process can be operated repeatedly for a certain period of time as long as required. In the meantime, the launderers register Ecash account with Internet bank and gain a cyber-wallet residing on their computer. The cyber wallet is an Ecash software. It can store and manage the launderer's coin, keeps records of all transactions, and makes the protocol steps appear as transparent as possible to the launderer [12].

Secondly the launderers transfer their illicit funds from each traditional bank account and deposit them into Ecash account through on line banking service. The launderers' computer as long as properly connected to the Internet can do all of this process. Once the illicit funds have been transferred to Ecash account, the cyber wallet would convert them into digital money (i.e., E-coin) legitimately and make them become untraceable and anonymous virtually. This is because that E-coin within Ecash system is unique in that it is minted by the client (e.g., the launderer) before being signed by the bank. E-coin has a serial number generated by cyber wallet. The serial number is blind and sent to the bank to be signed. The bank has no chance to see the serial number on the E-coin it signed.

In the integration phase, the launderers locating in any country or jurisdiction are able to access to digital funds from any unknown ISP in any country or jurisdiction by using Telnet (a basic command in the protocol for connecting to another computer host on the Internet). And then, the launderers either spend E-coin on real or personal property on line or have their Ecash account actually call the bank to transfer the funds to origin currency account or to the third country, thus concealing their true identity [2]. Figure 3 shows the Internet-based money laundering by means of Ecash. In Figure 3, Ecash withdrawing protocol allows the launderers' privacy to conduct Internet transactions. Therefore, the Internet bank that holds digital money and merchant that accepts E-coin have difficulty to identify the launderers. This would leave a longer trail for law enforcement agencies to follow. Though the use of E-coin to purchase luxury item is currently not very popular on the Internet, the temptation for retailers and money launderers seems growing as it is uneasy to trace who spent E-coin in the Internet.

RESEARCH METHODOLOGY

As the concept mentioned above, we believe that banking and financial institutions play an important role of anti-money laundering. Taiwan is an ideal location to examine the issue since Taiwan highly controls its foreign currency of outward/inward remittance, and is a founding member of the Asia/Pacific Group on Money Laundering since 1997. Senior bank operation managers were selected as participants. We believe that they are familiar with day-to-day operations and transactions that comply with Government's anti-money laundering policy and related company's regulations (e.g., cash transaction limit, transaction reporting limit, and relevant anti-money laundering process and procedures). To reduce a single source response bias, Government officials of Money Laundering Investigation Bureau were also selected.

We used the interview approach of Wintershield [19]. A qualitative interview approach enables us to capture and understand the phenomenon "how to prevent money laundering that adopts technology" (e.g., EFT is a type of technology as mentioned). Following Bunduchi's [4] rationale, the focus of our study is to search for happenings and not occurrences. Therefore, we attempt to understand the phenomenon (i.e., difficulties or issues of anti- Internet-based money laundering) in relation to Bank operations managers and relevant stakeholders' perception (i.e., Government officials) without necessarily looking for the statistical significance of findings. The common critique of qualitative design is the extent of its generalizability [5]. However, we attempt to understand a particular issue and not to just merely enumerate instances where a particular theory holds true [20].

The data were collected over a six-month period through the use of structured interviews. As previously mentioned, for broader examination of different stakeholders' perceptions, two groups of participants were used (Table 3). Group one was comprised of 15 bank operation managers and five operation managers from investment firms. It was worthwhile to examine how Taiwanese banking and financial institution operations managers have responded to issues and difficulties associated with the routines of anti-money laundering. Group two included ten Government officials form Money Laundering Investigation Bureau. Besides demographic questions, interview questions are shown in Table 4.

Table 3: Overview of Participants

Characteristics	Group One	Group Two
Institution	Banks Investment Firms	Money Laundering Investigation Bureau
Role of Institution	Payment gateway	Law Enforcement
Number of Participant	20	10
Participant	Senior operation manager	Senior supervisor and agent

Table 4: Selected Key Interview Topics

Guiding Topic of Interview	Purpose
Group 1: Operation manager	
Describe the current and future tendency of money laundering on the Internet	Ascertain the difficulties of anti-Internet-based money laundering
Explain and What are difficulties in operating anti-money laundering on the Internet	Ascertain the difficulties of anti-Internet-based money laundering
How do you view Internet-based money laundering as a potential risk to bank operation, and agree that technology applications and/or human intervention (e.g., KYC) frequently have effects on money laundering prevention? Explain the potential means of Internet-based money laundering and possible countermeasures	Identify possible countermeasures against such difficulties.
Group 2: Law enforcement agent	
Describe the current and future tendency of money laundering on the Internet	Ascertain the difficulties of anti-Internet-based money laundering
Explain and What are difficulties in enforcing law while dealing with money laundering on the Internet	Ascertain the difficulties of anti-Internet-based money laundering
Explain whether there are adequate administrative support and law against money laundering on the Internet	Identify possible countermeasures against such difficulties
Explain whether there is an appropriate Government support or international cooperative mechanism against money laundering on the Internet	Identify possible countermeasures against such difficulties

A 90-minute open-ended, in-depth interview was held with each participant in the two groups. Field notes were taken to record a detailed account of participants' thoughts, feelings, experiences, and perceptions throughout the research process [15]. Follow-up interviews were conducted to ensure that all necessary data were collected. With the prior consent of participants, tape recording was also used. More than 65% of participants had acquired considerable work experience in the context of anti-money laundering, law enforcement, and related policy making (Mean = 11 years). Overall, these participants were knowledgeable about their anti-money laundering routines. This reduces response bias.

FINDINGS AND DISCUSSION

Categorical aggregation was used to reduce and analyze the data. Our initial data list included two broad categories: concepts regarding the difficulties of anti-money laundering and concepts regarding counter-money laundering in the Internet. Based on these categories, we found nine difficulties that are embedded within the routines of anti-money laundering that can be managed to explore countermeasures. According to our interview data, the characteristics of the Internet technology appear to aggravate classic money laundering risk. This is indicated by over 80% of our participants that "*Internet is easy access . . . unphysical contact between the customer and the financial institution, remote control on any ISP, high privacy and rapid electronic transaction*." This raises several concerns in aspects of regulation, private right, technology and bank supervision covered in the following nine difficulties found.

Lack of Uniform Regulation

Our participants reported that "*law and some anti-money laundering rules are there but somewhat not clear to comply for Internet banking transactions. . .*". Despite that transactions performed by access to financial services through the Internet have revealed money laundering risk, the law that regulates the Internet banking and the new electronic payment technology is still vague. In Taiwan, the Act of 1997 only regulates conventional laundering and currently has no related initiative in anti-money laundering through the Internet.

This issue is also raised in the United States. In the United States, the purpose of the Money Laundering Control Act of 1986 is to avoid the launderers' structure cash transaction with domestic banks. Under that law, the financial institutions are obliged to file CTR and report suspicion. The US department of Treasury has established a technology-based law enforcement unit named FinCen (Financial Crimes Enforcement Network) to prevent and detect money laundering. Nevertheless, Ecash account offered on the Internet bank is not FDIC insured. That is, private vendor rather than Federal Reserve currently creates the digital money. Thus digital money would not affect monetary supply or policy yet. In this case, the non-FDIC insured Internet bank probably would not have mandatory compliance with the law. Furthermore, E-coin issuer may not be necessary a bank [3]. Thus, the law would be inadequate to regulate non-bank organizations.

Privacy Issues

We found that the privacy is a controversy while using lawful investigation into a suspicious violation of anti-money laundering regulation. As indicated by our participants, "*Taiwan law enforcement agency recently proposed to establish a Criminal Proceeds Flow Control Database that links with the host computer in every financial institution island wide. . .in that system, all customers' financial records would be revealed to the investigation authority*." This initiative has generated a privacy debate in Legislative Yuan. For example, the new electronic payment method with security protocol prevents individual's financial records from exposing to the open computer network. However before being convicted of money laundering, a question would be raised on that should an individual's financial privacy be protected when the law enforcement agency conducts investigation.

This finding is similar to that in Australia where electronic payment method such as stored value card is a concern about the control on collection and use of transaction and other data. The information may be valuable to the law enforcement agency. However, privacy right would be violated when disclose the information related to any particular use of the card where that particular use tries to identify the card user [16]. In the United States, the Privacy Act of 1974, the Right to Financial Privacy Act of 1982, and the Electronic Communication Act of 1986 are three principle laws to protect individual financial privacy. However, the standard to file a search is relaxed. Therefore, a balance between Privacy Act and anti-money laundering law should be considered [11].

Difficulty in Identification and Authentication

Our participants indicated that "*KYC (Know Your Customer) policy is to prevent traditional money laundering at the placement stage. In Internet banking, the risk is increasing because of reduction of personalized contact*

between the customer and the financial institution." When a bank account opened, it is a policy that the financial institution must verify the identity of a natural person or a business entity as well as verify the authentication of all documents and signature authority. However, through the Internet, the financial institution has difficulty to identify whether the bank account is opened on his own behalf. KYC policy may not be sufficient to authenticate the identity of the customer at the initial stage according to our participants.

In a sense, the launderers would take that advantage to conceal their true identity on the Internet. Specifically, the Internet banking makes KYC more difficult to identify whom actually uses bank account and from which location the account is accessed because of the fictitious identity and the mobile ISP worldwide. Our finding indicates a possible scenario of difficulty in identification and authentication that the launderers could enter an Internet bank through a distant ISP located in a country where high bank secrecy has and requires little documents for account opening in the name of someone else under control, and then process transactions through personal computer.

Another similar scenario is the use of ATM (Automatic Teller Machine) and phone banking services. They only need little information for identity verification and then conduct fund transfer without any direct physical interaction. Taiwan recently had an example indicating that phone banking service was used to transfer illicit funds generated from fraud activities under the cover of false Loan Service Company. This example is shared by one of our participants that "*a crime organization used a loan company to require victim deposit so-called guarantee money into bank account before false loan disbursement. Then transfer funds from victim's bank account to several third parties' bank accounts under his control by simply entering victim's PIN (Personal Identification Number) through telephone banking service online.*"

Low Transparency of Transaction

We found that low transparency of transaction can be a difficulty for anti-money laundering, particularly on the Internet. This is evidenced by our participants that "*secure cryptographic protocols ensure anonymous and untraceable records . . . the audit trials would be unclear to trace suspicious transactions that occur during the encrypted sales process when using Ecash online.*" In a sense, the law enforcement agency could be hindered to detect Ecash transactions in between initial subscription and final settlement during merchant's capturing process. As a result, it is unable to trace back the origin of illegal funds. A scenario is that money laundering indication for the Ecash would not be easy to establish, and thus the Internet bank and/or e-retailer may not fulfill reporting obligation if there is a substantial quantity of Ecash trading.

Our participants also reported that another laundering risk for the smart card (i.e., a case of Ecash application off line) varies based on operation characteristics that contain both open and closed-end systems. Open-end system indicates that money value can be directly transferred between cards. However, under closed-end system, money value can only be recharged from user's bank account and the used value would be directly credited to the merchant's bank account. The open-end smart card system such as Mondex (or MasterCard cash) could have higher risk because of allowing direct person-to-person value transaction without an intermediate bank involved. In that respect, the audit trial on transaction is insufficient. Our finding indicates a possible scenario that the launderers may use AVM (Automatic Vending Machine) or ATM to transfer illicit funds by means of purchasing the smart card and exchanging value anonymously. This low transparency of transaction increases money laundering risk on the Internet.

Rapid Growth of Technology for Organized Crime

Our participants reported that "*we reasonably assumed that organized crime may have solid resources to develop advanced technology in order to break encryption codes for the smart card, for example*." Therefore, this finding indicates a possible scenario that the launderers may crack the smart card's chip and modify the amount of money stored on it. As a result, the launderers could change the upper limit for the smart card value and circulate the funds in the form of electronic bits without passing through any regulated banking system. This is similar to that in the study of Sarigul [14] that launderers often use technology to abuse financial systems, leading to potential risk of money laundering on the Internet.

Jurisdictional Problem

We found that jurisdiction can be a problem as indicated by our participants that "*Internet has no boundary limitation . . .we are difficult to enforce anti-money laundering processes*." This is similar to that in other countries. For example, FATF remains a concern on determining jurisdiction for the licensing and supervision of financial services provided on the Internet. Within their own countries, the banking supervisors cannot ensure fi-

nancial services from the outside country servers comply with anti-money laundering procedures. The other issue arises in how to locate the place of the Internet transaction in order to decide which country or jurisdiction has the authority to investigate money laundering. Our finding indicates a scenario that the launderers might scatter their on-line transactions through various ISPs across different countries or jurisdictions, thus make trails longer to trace and circumvent the investigation because of confusion of the location that transactions taken place.

Web-Based Service Set Up by Organized Crime

We found that the launderers could layer their illicit funds under the cover of bogus or real information service provider and create an electronic payment channel for those funds. As our participants indicating, "*Under the guise of e-merchant, the launderers may take virtual order and provide service by collecting the illicit funds as payments through a seamless and labyrinthine network of the Internet banking service.*" Given that finding, Internet gambling seems an ideal Internet-based service to be a cover for the launderers. In this sense, all transactions can be performed by providing credit card information under fictional betting scheme. The server of this virtual casino could be maintained and located offshore in a lax anti-money laundering jurisdiction, thus make the law enforcement agency difficult to prosecute the relevant parties and collect transaction records.

Inability to Track the Internet Links

Our participants also argued that "*some Internet communication technology would hinder our ability to trace . . .*". For example, TCP (Transmission Control Protocol) allows data convey through the Internet by breaking down information into packets. Once the packets are created, IP (Internet Protocol) provides each packet with address information and direct it to the next destination on its travel between computer servers. In this sense, each transmission from a particular server should leave records on those servers with which it communicates. However, if a control log file (cookie) is not set up for a transmitted message and the IP address is not fixed for the user, then it may be difficult to determine the ultimate link between the launderers. Our finding indicates a possible scenario that the launderers may take advantage of the dial up connection that provides IP address on a temporarily basis by ISP. The launderers have the IP number while connected to the Internet. Once they completed illegal transactions and exited this connection, the IP number is assigned to the next active user. Thus, a specific launderer is difficult to determine.

Lack of Human Intervention against Money Laundering on the Internet

Our participants reported that "*it is difficult for human intervention against money laundering on the Internet*." Financial institutions have a responsibility under the anti-money laundering law, to be aware of the possibility that illegal activities may have occurred. Conventionally, bank employees through over-the-counter transactions can detect possible indications of money laundering activity. And they have an obligation to file suspicious report to the management for scrutiny. However, the lack of face-to-face interaction results in the difficulty of collecting conclusive evidence to determine whether it is money laundering by human judgment. Thus, money laundering risk in the placement stage on the Internet is increasing with less human intervention.

Our participants shared an example of the Internet banking service in Taiwan shows the deficiency of anti-money laundering procedure that can be implemented on line. In Taiwan, the Internet financial services include account enquiry, fund transfer, mutual fund subscription/redemption/switch, credit card payment and product information updates. For example, the extent of fund transfer services would depend on type of security protocol applied. For banks using SET protocol may provide inter-branch fund transfer with maximum amount limit of NTD 3 million (around USD 100,000) per day. On the contrary, for banks using SSL (SSL 128 bits) protocol, the inter-bank fund transfer is not allowed and in-house fund transfer to third party account is limited to NTD 100,000 (around USD 3,333) per day. Despite limited function of financial services, it would be an alternative for the launderers to structure illicit funds repeatedly for a certain period of time under current limitation.

Based on our finding, the critical issue would be that no human activity could monitor the frequency and trend of transaction on real time mode, thus the launderers may have sufficient time to layer transactions before they are found. Our participants mention that "*the most effective way to prevent money laundering is to catch the launderers in the act while structuring transactions*." This means that it would be more difficult to trace back to the origin after successful structure even if there is a completed but more complicated transaction records for the law enforcement agency. As indicated by the participants, to prolong investigation period and mess up the financial records are the purpose of the launderers.

Our participants also reported that "*writing computer money laundering detecting program for the Internet transactions . . .*". However, the launderers may figure out what criteria that are being judged by and as soon as change their laundering methods to avoid tracking. As a result, even when all computer procedures are obeyed, human beings are still better watchers when laundering is in process.

IMPLICATIONS

Based on the above findings, effectively, in order to prevent the Internet launderers, the key would be how to ascertain indication for possible money laundering activities on line, and then file suspicious transaction report or maintain financial records for law enforcement agency. Ideally, it seems computer program can perform this job. Nevertheless, as mentioned already, the launderers may learn existing rules applied and make a seemingly legal transaction pattern so as to evade attention from the computer program. Then the launderers would further take advantage of the Internet to sophisticate fund transfer routes and reduce the transparency of financial records.

Based on the findings, we argue that how to examine and control the working procedure while building initial account relationship with the customers would be a determinant that alleviates the risk of Internet-based money laundering. In a sense, the practical implication is shown in Figure 4 that illustrates the conceptual framework of countermeasures against Internet based money laundering. In the framework, we formulate three stages that consists of ascertain, control, and back-end operation support. Given our participants' suggestions and some literature, we provide principles and/or the best practices that should be considered to adopt in each stage. Stakeholders involved over the three stages are also shown. This framework can be a guideline for practitioners when setting up anti-Internet based money laundering mechanism.

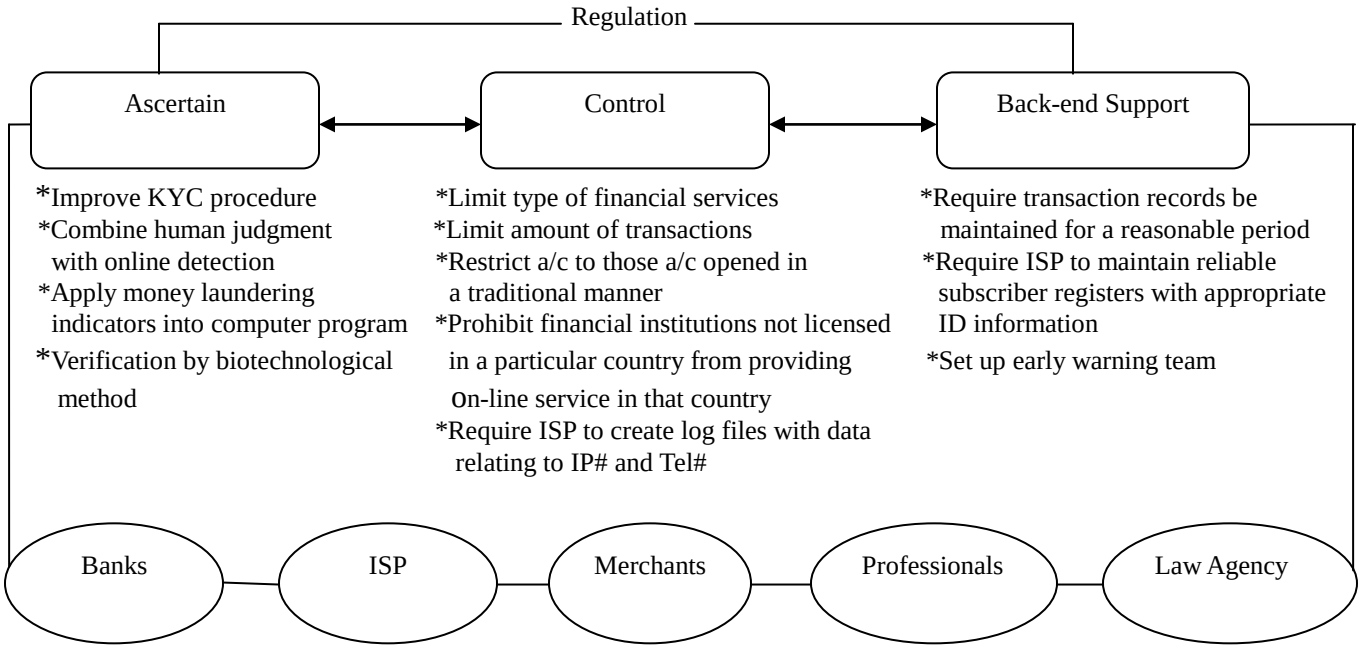

Figure 4: Conceptual Framework of Countermeasures against Internet-based Money Laundering

In the first stage of ascertain, KYC policy would be implemented by relevant business entities (e.g., banks) that provide Internet financial services. Conventionally, face-to-face customer identification, as a minimum, is a baseline anti-money laundering measure when the account is established. However, practically, because of market competition, depersonalized online account opening would be rendered to meet customer's convenience. In that respect, in order to reduce laundering risk while opening account through the Internet, financial institutions in selected countries adopt countermeasures as listed in Table 5.

Table 5 indicates that at first stage when building online business relationship with the bank, the KYC is conducted as it is in traditional way. However, the effectiveness of such countermeasure is still limited to whether frontline employee can acutely detect indications of money laundering and whether particular attention would be paid to those high-risk exceptional accounts. According to bank practice, it may accept account that is opened with incomplete documents (or other substitutes) on a deviation basis. However, it may generate a risk of temporary account as a conduit that the launderers would use to structure or collect illegal funds during the waiting period for collecting full documentations.

Despite the human judgment that may be cautiously exercised while establishing account, the difficulty of authenticating true ownership of bank account cannot be completely removed because of the characteristic of remote access to the account and thus conduct of transactions on behalf of true owner through the Internet. As a result, to more effectively safeguard the vulnerability of financial transactions in the Internet environment, some recommended principles that strengthen countermeasures such as KYC procedures, technical improvement, and transaction limitation are outlined in Table 6. It is noted that each of these principles has advantages and disadvantages.

Table 5: Current Countermeasures for Online Account Open in Selected Countries

Country	Countermeasures
Belgium	*Per anti-money laundering law, it makes no distinction between traditional and on-line account opening by fax, e-mail or Internet. A copy of probationary document must be filed and maintained by the entity.*
Japan	*Only accept on-line transaction of which account is opened through traditional face-to-face channel.*
Taiwan	*On-line transaction is currently limited to bank account that is already opened through over-the-counter procedure. No relevant law regulates on-line account open procedure.*
United States	*On-line account open procedure is similar to that by mail. The customer must enter identification number for verification.*

It is seen that the human judgment is a crucial factor for either traditional face-to-face or online account open when conduct money laundering prevention. However, in the middle of the transaction process, automated collection of objective information or at least in relation to certain rudimentary possible laundering indicators may be necessarily constructed, and assist either financial institution or law enforcement agency to timely and effectively trace suspicious transactions. The feasibility of biological verification on the account holder may be useful for the financial institution to verify the identity so as to discourage the launderers.

In the second stage of control, by limiting the range of online financial services and the amount of transaction, it may decrease the possible convenience of using financial institutions as an intermediary for money laundering. The availability of Internet service only limited to those accounts established in traditional way may reduce the variety of payment channel selected by the launderers. In case that financial institutions may establish website located in relaxed banking regulation region and then provide online financial service not allowed in home country, the firewall to block the access to such website may be constructed by regulating ISP as well as the log file to store IP number and telephone number for each user should be maintained for the law enforcement agency. Consequently, it can improve the ability to trace the Internet link.

In the back-end support stage, a compatible computer-based report in gathering and supplying significant financial transaction records and cross boarder wire transfer information should be readily useable by screening system for all relevant anti-money laundering parties. And all relevant intelligence covered by means of ISP through the Internet should be maintained for a reasonable period of time. An early-warning team is suggested to set up for every financial institution. The function of this team would review computer-based suspicious report and then make a tracking phone call to the account owner while discovering abnormal transaction patterns. The criteria for such scrutiny would be determined by the factors of amount, frequency, and purpose of transaction that would be regulated by law based on practical situation.

Table 6: Basic Principles for Potential Countermeasure

Principle

KYC procedure:

- *Strengthen existing customer identification requirement and revise procedures that can facilitate the expertise of financial institutions to truly know transaction pattern and financial behavior of nominal account holder over the life of business relationship.*

+ Advantage

- ✓ *By human scrutiny, as early as possible to detect abnormal pattern and conduct proper reaction.*
- ✓ *By periodical telephone contact and physical site visit on the customer, more or less, reduce the risk that the launderers take advantage of not necessary presence in the bank over the life of account, and then transacting illicit funds distantly.*

+ Disadvantage

- ✓ *Need experienced employee.*
- ✓ *Staff turnover and discontinuity of detecting money laundering training would influence the effectiveness of anti-money laundering measure.*
- ✓ *In respect to customer relationship management, the capacity per FTE (Full Time Employee) could be limited due to the concern on cost effective.*

Technical Improvement:

- *Develop advanced information technology that can detect suspicious on-line transaction.*

+ Advantage

- ✓ *Reduce bias from subjective human judgment.*
- ✓ *Reinforce accuracy of information by co-work with human-based monitoring*
- ✓ *Timely generate automated suspect report on daily, weekly or monthly basis*
- ✓ *Create explicit format for sorting, and then locate potential launderers as effectively as possible.*

+ Disadvantage

- ✓ *Need compatible computer report format that links to each relevant party.*
- ✓ *Need continuously revise money laundering criteria for computer program*
- ✓ *Need construct firewall to prevent the launderers from cracking the computer program*

- *Develop a new verification technology that may scan customer's physical characteristics such as eyeball, fingerprint and even DNA.*

+Advantage

- ✓ *Easily identify and authenticate true ownership of bank account*
- ✓ *Increase the difficulty of disguising identity, and then discourage the launderers.*

+ Disadvantage

- ✓ *Financial institutions and relevant parties may need sufficient database to store biological information. And the information exchange network that links with Bank, ISP, merchant, or even law enforcement agency is necessary to establish to cross verify the identity of true owner.*
- ✓ *Financially, cost effective would remain a concern*

Transaction Limitation:

- *To limit the type of on-line financial service or the amount of transaction*

+ Advantage

- ✓ *Reduce the alternative that the launderers may select*
- ✓ *Prolong the length of time that the launderers structure their illicit funds, thus probably discourage them.*

+ Disadvantage

- ✓ *Due to market competition, all financial institutions may not have uniform standard for the limitation of such financial services and transactions. Therefore, the launderers still could have selections to register in on-line banking that has relaxed limitation.*

As for countermeasures against Internet-based money laundering through smart card, it appears to be in need of uniform standard of fully accounted system for all various stored value cards to avoid peer-to-peer transactions (only limited to person to merchant or person to financial institution transactions). A practical implication is that a central database is recommended to build up for all transactions and thus makes it easier to reconstruct card balance and transaction history for the law enforcement agency to trace.

Based on our participants, to constrain the capacity of smart card including maximum value stored and turnover limits as well as number of smart cards per individual customer is adopted while issuing. For example, in Taiwan, regulation on stored value card allows maximum value of USD 300. And all accounting records should be kept for five years for the purpose of audit trial. Linking this new payment technology to bank accounts provides clear audit trials while using smart card online or offline mode. However, it should be noted that there would be a possible difficulty to establish international standard to such countermeasures, and then require uniform record keeping procedures for systems to enable the examination, documentation, and seizure of relevant records by investigation authorities.

Moreover, based on the findings, in order to achieve agreement on which country or jurisdiction would have authority to control anti-money laundering and conduct investigation, a practical implication can be referred to a recent joint Bank of France and French Banking Commission report [1] proposes to use a rule that the Internet transaction should be considered to have taken place in the computer that covers the financial service provider's information and management system. However, if ISP hosting provider's website is not in the same location as its management system where the account held, then the latter could be considered as the relevant location.

CONCLUSIONS AND LIMITATION

This study contributes to existing literature in two ways. First, it illustrates the above nine difficulties of anti-money laundering on the Internet. Second, this study illustrates a conceptual framework of countermeasures against Internet-based money laundering. We believe that such conceptualized countermeasures can be guidance for stakeholders such as law enforcement authorities, national legislators, and international financial institutions to achieve agreement on seeking to appropriate mechanism and/or law amendments to countermeasures. Based on our findings, the following paragraphs indicate significant attention in this study.

As mentioned, the current anti-money laundering law is not uniform to cover money laundering on the Internet. The Internet-based money laundering has been alerting the law enforcement agency that the Internet technology would be improving quickly and the launderers would use that Internet technology. In a sense, the law enforcement agency wishes to have access to all financial records. However, the private right would be violated. Despite no fully financial privacy right that can be protected while using so-called legitimate law enforcement inquiry into suspicious account, the future research may focus study on "should anonymous online transactions or all individual banking data be secretly monitored?" Such question would be a debate between legal authority, bank manager and relevant private right protection party.

In addition to traditional financial institution, ISP has become an important medium for the launderers. However, as for the responsibility of ISP, the current telecommunication law is inadequate to include their obligation to provide reliable user information. This results in that the appropriate regulation on ISP is in need. The legislative authority can opt to put more pressure on ISP as it does on the banking industry. In that sense, it may invoke serious attention from ISP to make electronic money laundering cumbersome.

Providing customers' quick banking services at any time and any place heavily relies on remote banking by means of the Internet technology. Given anti-money laundering regulation, financial institutions would use special investigatory software into computer systems so as to flag suspicious online transactions. Financial institutions would also establish early warning teams to timely monitor automated suspicious reports, thus detect money laundering indicators as reference to the probable cause to search by the law enforcement agency. And to reduce the potential risk of using temporary account by the launderers, financial institutions may refuse accepting incomplete documented account by restricting delegation authority in the frontline. However, the future research should be concerned with the extent of the implication of face-to-face account open procedure would be varied from country to country, and thus increase the risk of verification and authentication on the Internet. Bank employees training on verification and authentication would be helpful while business relationship established on the Internet. There would be a tendency to conduct account open online under certain limitations or at least as it does in traditional means.

Our three-stage framework include a wide range of concepts including regulation establishment (e.g., pri-

vate right protection, jurisdictional conflict, KYC procedures, transaction limit, etc.), technical improvement, and human judgment can be seeking for well-organized national and international co-operation among legislative authority, law enforcement agency, bank supervision, interior and exterior affairs, and ISP. However, we still argue that the counter Internet-based money laundering seems still be in the difficulty of covering all difficulties found above. Despite difficulties found and disadvantages for the possible countermeasures, the authorities would try every possible effort to hinder Inter-based money laundering activities.

In our framework, although the combined application of technology-based and human-based scrutiny may be feasible and effective to prevent money laundering; and revision on the law to cover Internet-based money laundering is a fundamental work to develop uniform law and international standard to combat Internet-based money laundering, KYC policy is always a baseline work when building online business relationship with customers. It should be noted that countermeasures cannot be mutually exclusive to use when examining Internet-based money laundering issues.

Lastly, limitation in this study should be noted that we only examined the phenomena of difficulties found for Internet-based money laundering, without necessarily looking for their statistical significance on the three-stage framework countermeasures as conceptualized above. However, a future research may consider the statistical significance.

REFERENCES

[1] Bank of France and Banking Commission (2006), *Internet: The Prudential Consequences*, 17.

[2] Bortner, R. M. (1996). Cyberlaundering: Anonymous Digital Cash and Money Laundering, a final paper for law and Internet, a seminar at the University of Miami School of Law, 3-4.

[3] Bosworth-Davies, R. (1997). *The Impact of International Money laundering Legislation.* London: FT Financial Publishing.

[4] Bunduchi, R. 2005. "Business relationships in Internet-based electronic markets: the role of good will trust and transaction costs", *Information Systems Journal*, vol.15, pp.321-341.

[5] Creswell, J. W. 1998, *Qualitative inquiry and research design*, Thousand Oaks, CA: Sage.

[6] FATF (2001), *Report on Money Laundering Typologies 2000-2001*, FATF Publishing.

[7] FATF(2003). New Anti-Money Laundering Standards Released http://www.oecd.org/daf/anti-bribery/newanti-moneylaunderingstandardsreleased.htm [June 22 2015].

[8] FATF (2009). Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors. www.oecd.org/tax/exchange-of-tax-information/43841099.pdf [June 22 2015].

[9] Intriago, C. A. (1991). *International Money Laundering*, A Eurostudy Special Report, London: EuroStudy Publishing Co., 5-10

[10] Internet World Stats (2013). Top 20 Internet Countries. http://www.internetworldstats.com/top20.htm [July 2015].

[11] Khan, G. S. (2011). Money Laundering Laws: and Their Effects on Individuals' Privacy. Lap Lambert Academic Publishing.

[12] O'Mahony, D., Pierce, M. and Tewari, H. (1997). *Electronic Payment Systems*, London: Artech House, 146-147

[13] Pegueros, V. (2012). *Security of Mobile Banking and Payments.* SANS Institute.

[14] Sarigul, H. (2013). Money Laundering and Abuse of the Financial Systems. *International Journal of Business and Management Studies*, 2 (1), 287-301.

[15] Silverman, D. (2000). *Theory in Qualitative Research*, Sage, London.

[16] Sneddon, M (1998). Elecronique Money in Australia. http://www.lex-electronica.org/articles/v2-2/sneddon.html

[17] Turban, E., Lee, J., King, D., & Chung, H. M. (2000), *Electronic Commerce: A Managerial Perspective*, New Jersey: Prentice-Hall.

[18] Welling, S. N. (1989). *Comments, Smurfs, Money Laundering and The Federal Criminal Law*, 41 Fla. L. Rev 287, 290 .

[19] Wintershield, B. C. (1994). "Building Capability from Within: The Insider's View of Core Competence." in *Competence-Based Competition*, eds Hamel, G. & Heene, A., New York: John Wiley & Sons.

[20] Yin, R. K. 1994, *Case Study Research Design and Methods*, Thousands Oak, CA: Sage.

ACKNOWLEDGEMENTS

This study was supported by the Bankers Association of the Republic of China in Taiwan.

AUTHOR BIOGRAPHY

Leelien Ken Huang is Associate Professor of Strategic Use of IT at Feng Chia University, Taiwan. His work focuses on the IT business value, cross cultural research issues in IS, mobile technology, and e-learning. He is currently studying IT executives' career and educational issues. Ken has ten years' experience in a banking managerial position. He is also the Founder Member of the Association for CIO Development Asia Pacific.