Winter 12-19-2001

Internet-Based Laundering

Leelien Huang

Hsiang-Hoo Ching

INTERNET-BASED LAUNDERING

Leelien Huang and Hsiang-Hoo Ching

Department of Public Finance, Feng Chia University

886-4-2451-7250, ext 2600

E-Mail: ken_l_huang@sinamail.com

pf_ching@fcu.edu.tw

ABSTRACT

Electronic commerce applications started with EFT (Electronic Fund Transfers) for large corporations, financial institutions, and a few small businesses in the early 1970s. Then, the development of EDI (Electronic Data Interchange) that expanded from financial system added this application to manufactures, retailers and services. In the early 1990s, the commercialization of the Internet had generated a number of potential Internet users rapidly. By 2008, the number of the Internet user is predicted to reach 750 million globally according to Forrest Research Institute in 1996. 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.

PREAMBLE

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 is not inside of normal economic activity and statistics. [1] 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 [2] 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. FATF developed Forty Recommendations that set out measures for member countries to implement anti-money laundering policy. [3] Many non-FATF member countries have recognized Forty Recommendations as international standard for anti-money laundering and initiate their own countermeasures. [4]

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 attempts to illustrate classic and Internet-based money laundering schemes and will explore potential loopholes that occur on web-based laundering. This paper also reviews counter money laundering initiatives and issues for money laundering through the Internet. Finally, the framework of anti-money laundering through the Internet will be addressed so that the law enforcement authorities, national legislators, and international organizations may achieve agreement on seeking for appropriate amendments to countermeasures against Internet-based laundering.

CLASSIC APPROACH FOR MONEY LAUNDERING

Money laundering is the approach of hiding the illicit source or illicit application of income, and then transforming that income to be legitimate. [5] 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. In that respect, it consists of three basic phases. [6]

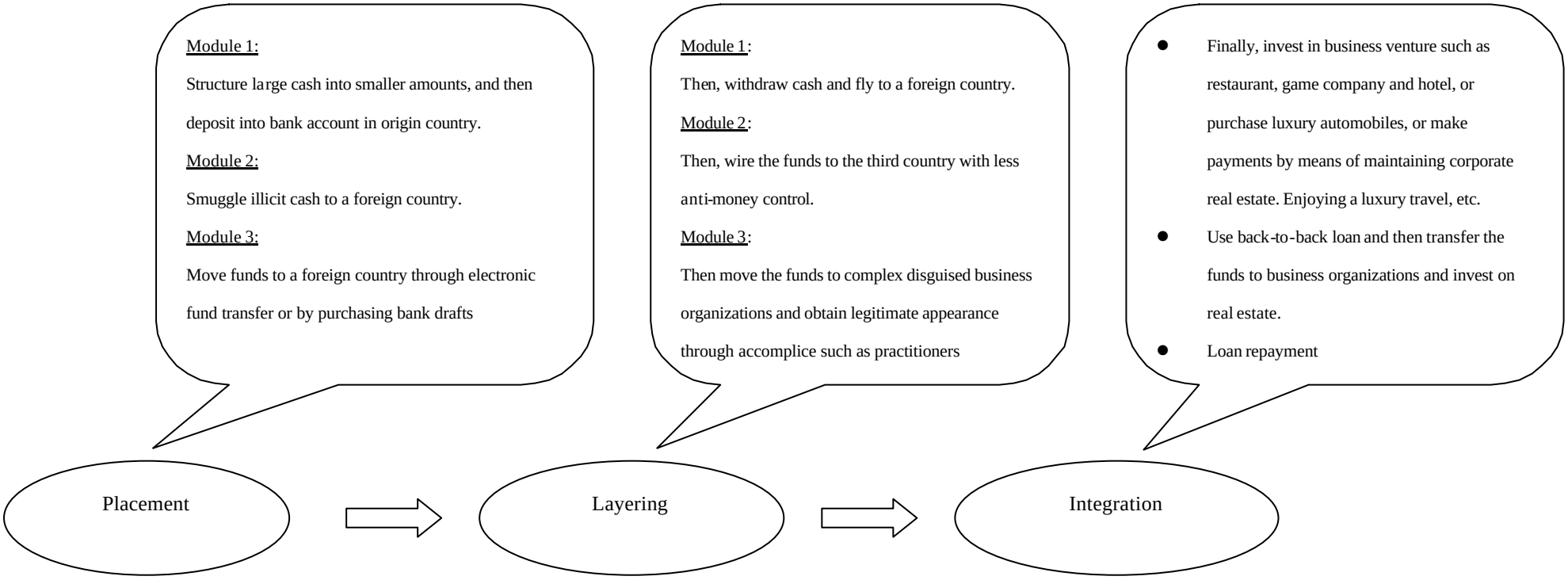
In the beginning placement phase, the launderers deposit their illegal activity proceeds into the financial system. In order to avoid detection, the large sum of tainted proceeds might be divided into less conspicuous smaller amounts that fall beneath bank regulatory reporting limit [7] and then deposited 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 will 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. [8] 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. The module for classic money laundering is depicted in the Figure 1.

In the 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 [9] 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

Figure 1 The Selected Typical Module for Classic Money Laundering



adequate financial infrastructures and transit bank accounts through withdrawing cash [10] or wiring at various locations. 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 will 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 classic module described here 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 website based transaction to avoid detection gains a loyal following.

MONEY LAUNDERING SCHEME ON THE INTERNET

As stated in this paper, convenience and anonymity are attractiveness to the launderers. Internet access has these features. The probability of using the Internet as a laundering channel might be high since the Internet has grown dramatically from its inception in the late 1970s to today's truly global medium. [11] 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 [12] were being developed to protect confidentiality and authentication. [13] 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 more difficult to examine the launderers' identification and give an appealing opportunity to them. Consequently, cashless payment and remote laundering through the Internet will come to be the new type of detergent that allows for cleaning dirty money.

Eventually, the idea of money laundering electronically is not a new one. A typical example of cashless payment is electronic fund transfer (EFT) [14] that has been mostly used to possess a nearly risk free conduit for moving money between countries. This illicit fund transfer with limited information regarding the party involved [15] can be easily hidden because of large wire transactions occurring daily in the United States, [16] for example. More explicitly, the Table 1 shows non-cash payments that may be preferred by the launderers.

Basically, the launderers will employ electronic cashless payments as illustrated when conducting money laundering through the Internet. Following the continuous growth of on-line banking facilities, [17] the launderers can easily open bank account with fake registered identity on any ISP (Internet Service Provider) 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. The Table 2 indicates selected items mostly purchased on line and probably used by the launderers to make the illicit funds appear legally.

Specifically, credit card is the most popular payment method for cyberspace shopping today. An example of Internet-based 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

Table 1 Technology-Based Payment Attraction to Money Laundering

Payment Instrument	Medium	Status
Credit Card	POS (Point of Sale)	On-Line
	EDC (Electronic Data Capture)	On-Line
	Imprinter	Off-Line
ATM card/ Check Card	Auto Teller Machine	On-Line
Stored Value Card (Smart card)	POS	Off-Line
Paper Check	ACH / VAN	On-Line
EFT	CHIPS	On-Line
Digital Cash [18]		On-Line

Table 2 Items Purchase On Line (Number of Respondents: 645) [19]

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.*

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, IIS (Internet Invoice Service), CA (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. [20] Thus, it makes transactions more difficult to trace.

Another example of Internet-based laundering would be the use of Ecash. Ecash was developed by DigiCash [21] that is a Holland and the United States based company to allow fully anonymous secure electronic cash to be used on the Internet. The security is improved by extensive use of both symmetric and asymmetric (digital blind signature techniques) cryptography required for open computer network. Ecash worth real monetary value has been available on the Internet since October 1995. [22] Hence, Ecash may become a particular interest to money launderers and law enforcement authorities because of its unconditionally untraceable trait.

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 mean time, the launderers register Ecash account with Internet bank and gain a cyber wallet [23] residing on their computer. 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 (called E-coin) legitimately and make them become untraceable and anonymous virtually. [24] 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. [25] 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. [26] The Figure 3 shows the Internet-based laundering by means of Ecash. In the 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 [27] and money launderers seems growing as it is uneasy to trace who spent E-coin in the Internet.

ISSUES ON THE INTERNET-BASED LAUNDERING

The characteristics [28] of the Internet technology appear to aggravate classic money laundering risk. Several concerns are raised and covered by aspects of regulation, private right, technology and bank supervision.

Lack of Uniform Regulation

Transactions performed by access to financial services through the Internet have revealed money laundering risk. However, the law that regulates the Internet banking and the new electronic payment technology is vague. For example, in the United States, the purpose of the Money Laundering Control Act of 1986 [29] is to avoid the launderers' structure cash transaction with domestic banks. Under that law, the

Figure 2 Internet-Based Laundering by Credit Card Payment

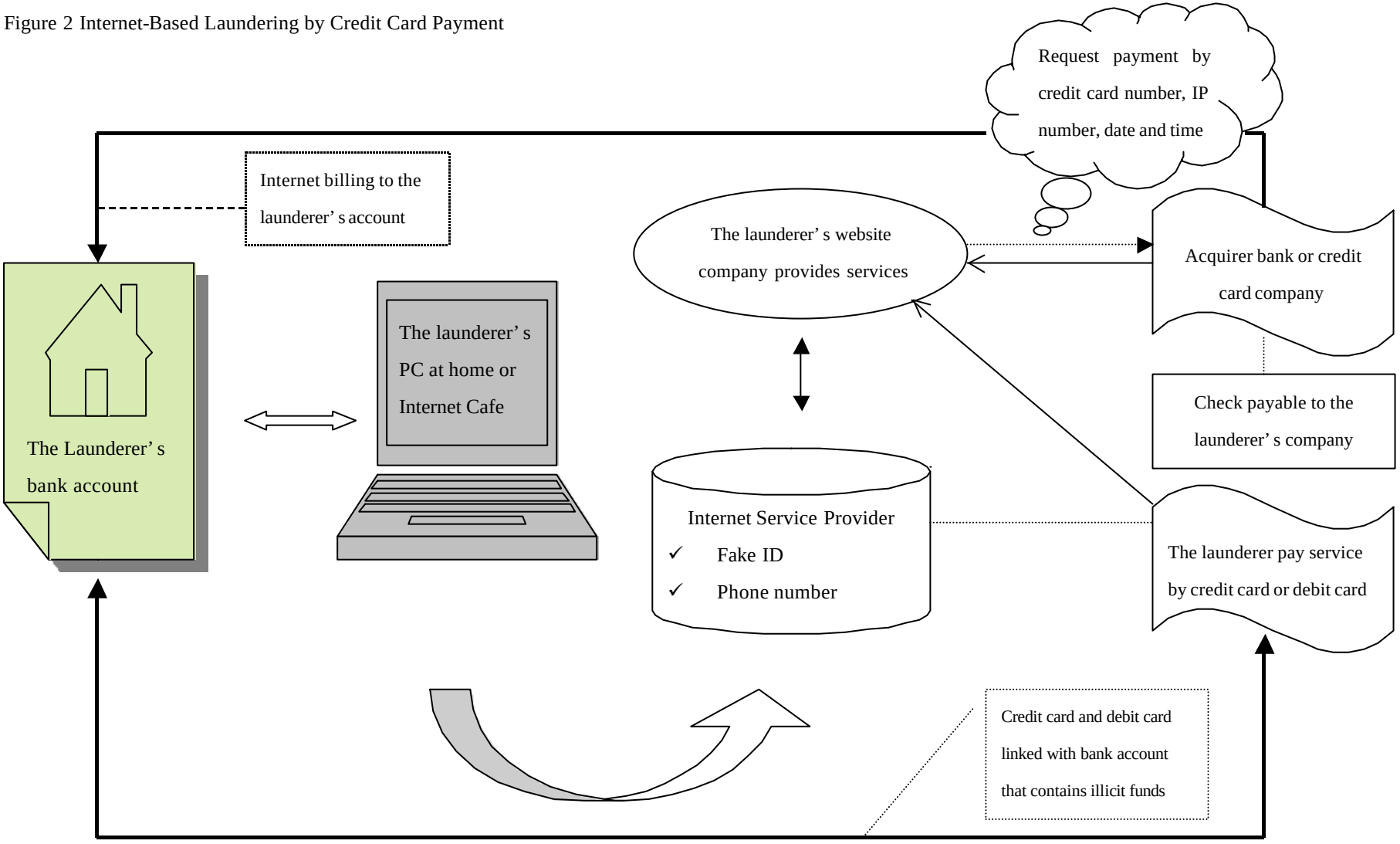
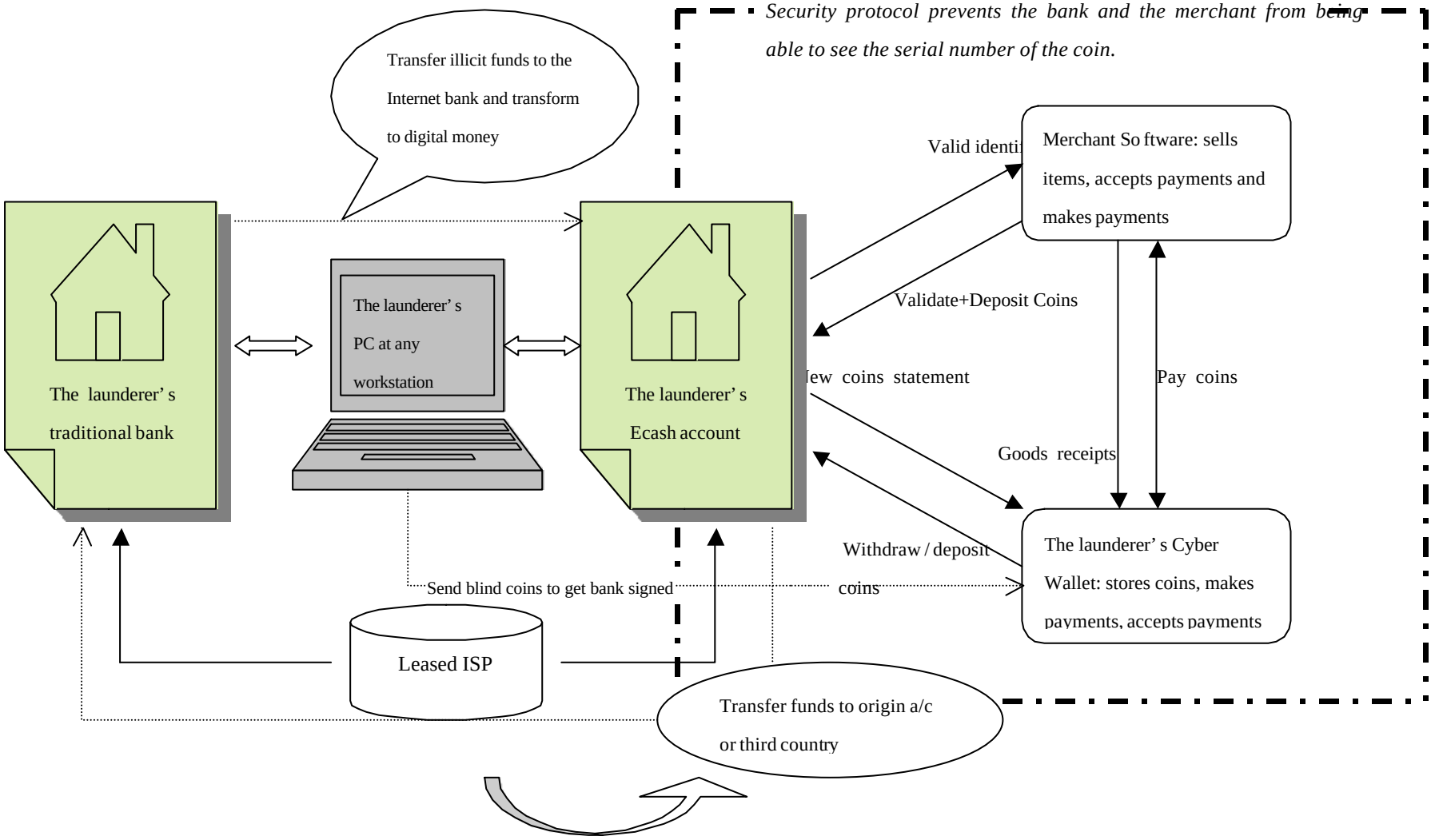


Figure 3 Internet-Based Laundering by Ecash



financial institutions are obliged to file CTR and report suspicion. [30] Nevertheless, Ecash account offered on the Internet bank is not FDIC insured. [31] The non-FDIC insured Internet bank probably would not have mandatory compliance with the law. [32] Furthermore, E-coin issuer may not be necessary a bank. [33] Thus, the law would be inadequate to regulate non-bank organizations. In Taiwan, the Act of 1997 only regulates conventional laundering and currently has no related initiative in anti-money laundering through the Internet.

Privacy Issues

The privacy is a controversy while using lawful investigation into a suspicious violation of anti-money laundering regulation. The new electronic payment method with security protocol prevents individual's financial records from exposing to the open computer network. Before being convicted of money laundering, a question will be raised on that should an individual's financial privacy be protected when the law enforcement agency conducts investigation.

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.

In Australia, an example of electronic payment method such as stored value card is also 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 will be violated when disclose the information related to any particular use of the card where that particular use try to identify the card user. [34] Consequently, a balance between Privacy Act [35] and anti-money laundering law should be considered.

Difficulty in Identification and Authentication

KYC (Know Your Customer) policy [36] is implemented to prevent traditional money laundering at the placement stage. However, in the example of Internet banking, the risk is increasing because of reduction of personalized contact between the customer and the financial institution. In other words, through the Internet, the financial institution has difficulty to identify whether the bank account is opened on his own behalf. Moreover, KYC may not be sufficient to authenticate the identity of the customer at the initial stage. 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.

One scenario showing difficulty in identification and authentication is that the launderers could enter an Internet bank through a distant ISP located in a country where has high bank secrecy and requires little documents for account opening in the name of someone else under control, and then process transactions through personal computer.

Another similar on line 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. [37]

Low Transparency of Transaction

Secure cryptographic protocols ensure anonymous and untraceable records. It means that the audit trials would be unclear to trace suspicious transactions that occur during the sales process. In the example of the nature of Ecash, 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 warning scenario is that money laundering indication for the Ecash would not be easy to establish, and thus the Internet bank and e-retailer may not fulfill reporting obligation if there is a substantial quantity of Ecash trading in the near future.

The laundering risk for the smart card, another case of Ecash application off line, varies based on operation characteristics: open and closed-end system. [38] The open-end smart card system such as Mondex [39] 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. A possible scenario is 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.

Rapid Growth of Technology for Organized Crime

It is reasonably assumed that international organised crime may have solid resources to develop advanced technology in order to break encryption codes for the smart card. Thus, a scenario is that the launderers may crack the smart card's chip and modify the amount of money stored on it. Consequently, 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.

The Issues of Jurisdictional Problem

Recently, 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 financial services from the out side 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. A scenario would be 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. [40]

Web-Based Service Set Up by Organized Crime

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. A scenario is that 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 scenario, Internet gambling [41] seems an ideal Internet-based service to be a cover for the launderers. In the case of the Internet gambling, 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

TCP (Transmission Control Protocol) allows data convey through the Internet by breaking down information into packets. Once the packets are created, IP (Internet Protocol) [42] provides each packet with address information and direct it to the next destination on its travel between computer servers. Consequently, 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.

A scenario is 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

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. [43] Thus, money laundering risk in the placement stage on the Internet is increasing with less human intervention.

An example of the Internet banking service recently launched by local banks in Taiwan shows the deficiency of anti-money laundering procedure that can be implemented on line. Despite limited function of financial services [44] at initial stage, it would be an alternative for the launderers to structure illicit funds repeatedly for a certain period of time under current limitation. The critical issue will be that no human activity could monitor the frequency and trend of transaction on real time mode, [45] thus the launderers may have sufficient time to layer transactions before they are found.

Another example is 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.

COUNTERMEASURES AGAINST INTERNET-BASED LAUNDERING

Effectively, in order to prevent the Internet launderers, the key issue 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. In view of 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 banking laundering.

Framework of Countermeasures Against Internet-Based Laundering

The Figure 4 illustrates the foundermental framework for counter Internet based laundering. The framework consists of ascertain, control, and back-end operation support.

Firstly in the stage of ascertain, KYC policy would be implemented by relevant business entities that provide Internet financial services as shown in the Figure 4. 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 on-line

account opening would be rendered to meet customer's convenience. In that respect, in order to reduce laundering risk while open account through the Internet, financial institutions in different countries have countermeasures listed in the Table 3, for example.

Table 3 indicates at first stage when building on-line business relationship with the bank, the KYC is tried to conduct as it does in traditional way. However, the effectiveness of such measure is still limited to whether front-line employee can acutely detect indications of money laundering and whether particular attention would be paid to those high-risk exceptional accounts. [46]

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, recommended principles of potential solutions that may reinforce current countermeasures be outlined in the Table 4. It is seen that the human judgment is a crucial factor for either traditional face-to-face or on-line 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 on-line 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 on-line 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 will be determined by the factors of amount, frequency, and purpose of transaction that would be regulated by law based on practical situation.

Possible Solutions for Smart Card

As for countermeasures against 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 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. To constrain the capacity of smart card

Figure 4 Framework of Counter Internet Based Laundering

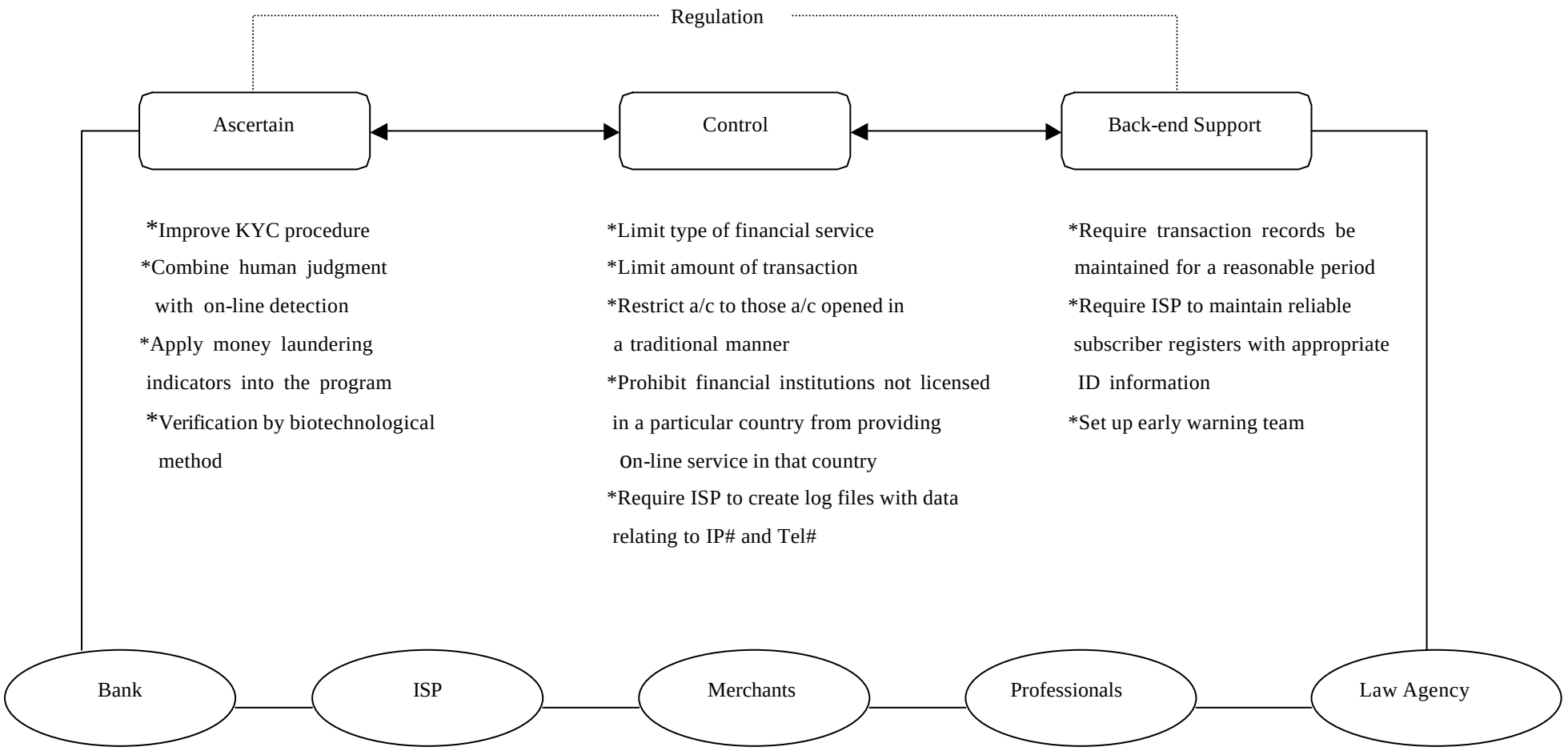


Table 3 Current Countermeasures for On-Line Account Open by Selected Countries

Country	Measure
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.*

Table 4 Basic Principles for Potential Countermeasure

Principle
By 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.*

Table 4 Basic Principles for Potential Countermeasure (Con' d)

Principle
By 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*
By 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.*

including maximum value stored and turnover limits as well as number of smart cards per individual customer is suggested while issuing. [47] Linking this new payment technology to bank accounts is also feasible to provide clear audit trials while using smart card on-line or off-line mode. Certainly, 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.

Jurisdictional Issues

In this regard, in order to achieve agreement on which country or jurisdiction would have authority to control anti-money laundering and conduct investigation, a recent joint Bank of France and French Banking Commission report 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. [48]

CONCLUSION

In comparison with classic money laundering technique, electronic money laundering scheme takes advantages of remote access, quick fund transfer and highly secured transaction in the Internet. Despite the absence of data showing the magnitude of the Internet-based laundering, we must accept that we currently traversing a period of transition to electronic means of money laundering. The examples given in this article are only typical modules that the launderers may use. From the examples illustrated, they tell us the efficiency of electronic payment method and the application of security protocol in the Internet are abused by the launderers to legitimize criminal proceeds. However, the current anti-money laundering law is not sufficient to cover money laundering in the Internet. The Internet-based laundering has been alerting the law enforcement agency. It is assumed that the law enforcement agency would think of ways to surpass the advances of the Internet-based laundering so as to catch money launderers in the act. Nevertheless, in a free market, it is inevitable that the Internet technology will be improving quickly and the launderers would use that Internet technology. As a result, prohibiting Internet transaction on the grounds that such transactions are difficult to trace is not basically feasible. Thus, it is summarized that:

1. From the point of view of the law enforcement agency, they worry that the Internet may become the launderers' paradise. In that respect, the law enforcement agency wishes to have access to all financial records. The private right would be violated under that expectation. Despite no fully financial privacy right that can be protected while using so-called legitimate law enforcement inquiry into suspicious account, should anonymous on-line transactions or all individual banking data be secretly monitored? Such question would be a debate between legal authority, banking supervisor and relevant private right protection party.

2. In the era of the Internet environment, in addition to traditional financial institution, ISP has become an important medium for the launderers. 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 regard, it may invoke serious attention from ISP to make electronic money laundering cumbersome.

3. From the point of view of the financial institutions, obviously, most honest citizens are the target groups that

the financial institutions will deal with. The financial institutions would be continuously seeking for advances in product developing and financial service upgrade. To provide customers' quick response on banking services at any time and any place is heavily relying on remote banking by means of the Internet technology. As a result of compliance with anti-money regulation, they would be convinced to implement special investigatory software into their computer systems so as to flag suspicious on-line transactions. The financial institutions probably would 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 in order to reduce the potential risk of using temporary account by the launderers, the bank is practical to refuse accepting incomplete documented account by restricting delegation authority in the frontline. The extent of the implication of face-to-face account open procedure will be varied from country to country. However, there would be a tendency to conduct account open on-line under certain limitations or at least as it does in traditional means. Bank employee training on verification and authentication would be reinforced while business relationship established in the Internet. Consequently, more or less, the loopholes are to be avoided so that the financial institutions may alleviate the possibility of being limitless conduits for the launderers to move money between countries.

4. Many issues will be experienced before the entire anti-money laundering system settles down to cover this revolutionary mode of money laundering. In view of those mentioned issues and to find out feasible solutions, a wide range of disciplines including regulation establishment, private right protection, jurisdictional conflict, technical improvement and human judgment are currently seeking for well-organised national and international co-operation among legislative authority, law enforcement agency, bank supervision, interior and exterior affair, and ISP. The counter Internet-based laundering seems still be in the difficulty of covering all mentioned issues. Despite those issues and disadvantages for the possible countermeasures, the authorities would never stop trying to crack down the criminals. They would try every possible effort to hinder money laundering activities. Many multi-ways of possible solutions to prevent money laundering need to be reviewed and reinforced periodically since the technology behind the new electronic payment system is still developing. However before well-thought countermeasures fully developed, at least, the anti-money laundering law should be amended to cover Internet-based laundering, and thus comply all relevant parties in the economy system.

5. If the launderers can take advantage of the Internet technology to legitimate the illicit funds, same way may be used in the anti-money laundering measures. Specifically, the combined application of technology-based and human-based scrutiny may be feasible and effective to prevent money laundering. However, which part that is more focusing would be varied from case to case.

6. Revision on the law to cover money laundering in the Internet environment is a foundermental work to develop uniform law and international standard to combat Internet-based laundering. And no matter how much better improved is anti-money laundering measure; KYC policy is always a very baseline work when building on-line business relationship with customers.

REFERENCES

[1] IMF stated that the aggregate size of money laundering in the world is approximately accounts for tow to five percent of world GDP, see IMF Statistics in 1996. According to United Nations Statistics Division and FATF on Money Laundering 2001, global money laundering

volume is estimated from USD 531 billion to USD 1.46 trillion, which are the size for Spain and United Kingdom respectively.

[2] A reputation for integrity is one of the most of valuable assets of financial institutions.

[3] Member of the FATF include 29 countries and jurisdictions including the major financial institution in countries of Europe, North and South America, and Asia as well as the European Commission and the Gulf Co-operation Council. More details for Forty recommendations see www.oecd.org.

[4] International organizations such as the United Nations, Bank for International Settlements have taken initial steps to address money laundering issues in 1980s. Regional groups such as the European Union, Council of Europe, and Organization of American States established counter money laundering standards for their member countries. The Caribbean, Asia and South Africa have structured counter money laundering task force. And similar groups will be also planned for Latin American and western Africa in the near future. See www.oecd.org.

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

[6] Intriago, Charles A., International Money Laundering, (A Eurostudy Special Report, London: Eurostudy Publishing Co., 1991), 5-10

[7] For example, USD 10,000 is the reporting limit to file Currency Transaction Report under 31 C.F.R. sect. 103.22(a)(1), the Bank Secrecy Act of the United States. In Taiwan, NTD 1,500,000 (USD 43,478 equ, 1:34.5) is requirement that Large Currency Transaction Report filed under Money Laundering Control Act of 1996.

[8] The launderers might simply wire the illicit funds through a series of bank accounts worldwide. This method to disperse bank accounts at various locations is quite prevalent for those countries and territories where counter money laundering policy is weak.

[9] In fact, banking system plays a role to prevent money laundering by conducting ethical principles that banking supervisors to ensure their employees to comply with anti-money laundering program.

[10] The launderers may also purchase negotiable certificates such as travel's check, NCD, international money order, bond and stock to make transactions complicated and difficult to trace.

[11] More than 25 million Americans had Internet access in early 1995. See Legal Issues in the World of Digital Cash, http://www.info-nation.com/cashlaw.htm1/. By the end of last century, after a period of exponential growth, the number of host computers had grown to 16 million. If each of host computers is used by 10 persons, there are 160 million populations who have access to services in the Internet. See Internet Host Count maintained by the Network Wizards, Menlo Park, California. In Taiwan, there are approximately 0.6 million Internet users.

[12] These electronic payment methods are covered by EFT (Electronic Fund Transfer) and debit card such as ATM card, stored value card such as Mondex and VisaCash, credit card based payment, Ecash and Echeck.

[13] 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.

[14] For instance, 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 Fedwire that is something like that called IBRS (Inter-Bank Remittance System) in Taiwan.

[15] See 31 U.S.C. sect. 5313 (1988); 31 C.F.R. sect. 103.22 (1988).

[16] Approximately, there are 700,000 wire transfers happen daily in the United States alone. This accounts for about USD 2 trillion. See Office of Technology Assessment, Congress of the United States, Information

Technology for the Control of Money Laundering, iii (1995) (OTA-ITC-630).

[17] The range of financial services available through the Internet includes direct payment, EFT, issue of checks, subscription of bond, security, and mutual fund, credit card cash advance, and open/closing of bank accounts.

[18] Digital cash has been defined as a series of numbers that have an intrinsic value in the form of currency. See David Cline, Cryptography Protocols for Digital Cash, Term Paper, School of Engineering and Applied Science (Computer Security I), George Washington University. Also available on: http://www.seas.gwu.edu/student/clinedav/.

[19] Complied form the Graphics, Visualization and Usability (GVU) Center 10th WWW User Survey 1998, Georgia Institute of Technology. Also available on http://www.cc.gatech.edu/gvu/user_surveys. Quoted from Efrain Turban, Jae Lee, David King, H. Michael Chung, Electronic Commerce: A Managerial Perspective, (New Jersey: Prentice-Hall, INC., 2000).

[20] See FATF, Report on Money Laundering Typologies 2000-2001, February 2001.

[21] See DigiCash web server, 1996, http://www.digicash.com/.

[22] Mark Twain bank of St. Louis started issuing Ecash in U.S dollars. See Mark Twain Bank web server, St. Louis, MO, 1996, http://www.marktwain.com/.

[23] 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. See Donald O'Mahony, Michael Pierce, Hitesh Tewari, Electronic Payment Systems, (London: Artech House, 1997), 146-147

[24] To use E-coin within Ecash system is unique in that it is minted by the client (the launderer) before being signed by the bank. Each 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. Thus, E-coin is untraceable and anonymous. Ibid., 148

[25] Telnet is a basic command in the protocol for connecting to another computer host on the Internet.

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

[27] In the United States, cash transaction over USD 10,000 is subject to transaction filing requirement for the retailers. See 18 U.S.C.sect. 5311-5316 (Supp. IV 1986); 31 C.F.R.sect.103.22(a)(1)(1988).

[28] The characteristics of the Internet technology are easy access through the Internet, unphysical contact between the customer and the financial institution, remote control on any ISP, high privacy and rapid electronic transaction.

[29] The amendments to the Bank Secrecy Act of 1970.

[30] The US department of Treasury also has established a technology-based law enforcement unit named FinCen (Financial Crimes Enforcement Network) to prevent and detect money laundering.

[31] In the United States, private vendor rather than Federal Reserve currently creates the digital money. Thus digital money will not affect monetary supply or policy yet. R. Mark Bortner, op.cit., 4

[32] R. Mark Bortnet, op.cit., 4

[33] In practice the operation of an Ecash system may be easily conducted by any entity that has the infrastructure in place. See Rowan Bosworth-Davies, The Impact of International Money Laundering Legislation, (London: FT Financial Publishing, 1997), 162

[34] See Mark Sneddon, Elecronique Money in Australia, http://www.lex-electronica.org/articles/v2-2/sneddon.html.

[35] Currently, 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.

[36] 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.

[37] This example is cited 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.

[38] 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 will be directly credited to the merchant's bank account.

[39] The Mondex payment scheme was developed by Natwest in 1990. Its first trial in 1992 was launched for 6,000 staff at Natwest in London. Then in 1995, a major public trial was conducted in Swindon. In July 1996, Mondex International was formed.

[40] Despite no such evidence, it cannot be considered there is no sign of that laundering occurring on the Internet. It is believed that the methods to detect this type of Internet-based laundering activity have not been developed. See FATF, Report on Money Laundering Typologies 2000-2001, February 2001.

[41] According to FATF report, there is evidence in some FATF member countries that the launderers are using the Internet gambling to launder the proceeds of crime.

[42] All e-mail address and websites have a unique IP number consisting of four numbers ranging from 0 to 255. The IP number is separated by periods and can be indicated as the mailing address of the computer to which the content is being sent.

[43] The banking employee has knowledge of any attempted structuring by the launderers. Thus it appears that the ability to launder the illegal profits would be hampered.

[44] As of August 2001 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 will 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 (USD 86,956 equ, 1:34.5) 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 (USD 2,899 equ, 1:34.5) per day.

[45] The most effective way to prevent money laundering is to catch the launderers in the act while structuring transactions. 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. To prolong investigation period and mess up the financial records are the purpose of the launderers.

[46] According to bank practice, it may accept account that is opened with incomplete documents (or other substitute) 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.

[47] In Taiwan, regulation on stored value card allows maximum value of NTD 10,000 (USD 290 equ, 1:34.5). And all accounting records should be kept for five years for the purpose of audit trial.

[48] See Bank of France and Banking Commission, Internet: The Prudential Consequences, 5 July 2000, 17