Money Laundering in Cyberspace

Minwoo Yun, Ph.D.
Assistant Professor
Hansei University
Money laundering is...

- Clean dirty money (money obtained from illegal or dubious sources) into clean money
- Inject money originated from questionable sources into the legitimate (or legal) financial system
- Hide questionable origin of money obtained from various illegal or illegitimate activities
- Transfer money outside the legitimate regulations such as government, bank,...etc. for the purpose of tax avoidance, hiding sources of money, and/or criminal or terrorist activities
Money laundering usually means...

- For organized criminals/traffickers,
  1) hide illegal origins of a large sum of cash earned from criminal activities
  2) money ended up in the legitimate financial system in various forms...
  3) a substantial amount of money involved

- For terrorists,
  1) hide sources of money for terrorist attacks
  2) transfer money into terrorist operatives who actually prepare for a particular terrorist attack
  3) a rather small amount of money involved for consumption
Money laundering is NOW...

- $200 billion is successfully laundered across the world each year...
- The amount of money laundered yearly is as high as $100 billion in the U.S. and $300-500 billion worldwide (The U.S. Department of Treasury)
- The number ranges between $600 billion and $1.5 trillion (Financial Action Task Force on Money Laundering)
- (One million seconds = eleven and a half days/ One billion seconds = thirty-one years)
In 2001, Federal Reserve Bank of New York calculated that there was more than $800 billion on deposit in Grand Cayman (this amount is increasing at a rate of $120 billion each year).

That is equivalent to:
- twice the amount of money on deposit in all of the banks in New York city
- nearly 20 percent of all of the deposits in the U.S.
- $3000 for each man, woman and children in the U.S.
Process of Money Laundering: Organized criminal case

- Money ended up in the legitimate financial system such as banks, stocks, securities, real estates...
- Typically summarized in three stages
  1) Placement
  2) Layering
  3) Integration
Process of Money Laundering: Terrorists case

- Hawala, Hawallah, hundi, fei-chen...
- Underground banking system
- Trust-based traditional system

- A customer in country A → A hawalladar in country A → A hawalladar in country B → A customer in country B; later, two hawalladars in country A & B cancel each other out.
Off-line money laundering

- Smurfing (under $ 10,000)
- Import/export trading business
- Black Market Peso exchange (BMPE)
- Offshore banks
- Infiltration of Banks, Insurance, & Securities
- Own your own bank
- Running cash based business such as restaurant, casino, Laundromat, gold & jewellery, retail outlets and consulting firms,...
Cont.

- Art & antique dealers
- Bureau de change shops
- Hotels, bars, night-clubs, video rental companies, vending machine operators, parking lots
- Underground banking system such as hawalla
- + identity theft, accomplice, blackmail, bribe, front company, honey-trap (espionage technique), fraud, ...
Money-wash in cyberspace

- Basically, money-wash in cyberspace is not much different from that in offline.
- In most cases, cyber-money laundering is combined & integrated with offline-money laundering.
- Only uniqueness about cyber money laundering is cyber itself (in cyberspace and/or by means of computer tech.)
What is unique about cyberspace?

- High anonymity
- High secrecy
- More difficulty of law enforcement, meaning more security for crooks (due to lack of regulations)
- Less cost & efforts
- SPEED!!!

Thus, more and more crooks are turning into cyberspace for their criminal abuse, as offline is more and more strictly regulated by legitimate authorities worldwide (more banking regulations, hard-pressure on jurisdictions hosting offshore banks)
Money-wash businesses in Cyberspace

- Internet-based gambling operations

- Internet banking (Ecash, Digital cash, e-gold, anonymous account, prepaid card, etc...)
From an American perspective, cyberspace banks operate differently from commercial banks in the following fundamental aspects:

A. They do not accept deposits as those transactions are understood in the US.
B. They do not have bank charters from federal or state governments.
C. They do not have federal deposit insurance protecting the accounts.
D. They are not subject to federal or state regulation.

Cyberspace banking can provide payments for purchases over the Internet and other such services, a process that is growing rapidly. Cyberspace banks act as intermediaries in transactions involving the sales of goods, computer software, and presumably financial information and services. Their potential roles in transactions extend as far as the imagination.

http://www.subcontinent.com/sapra/bulletin/96feb-mar/si960308.html
The following innovations are underway on the Internet:

* Digital cash allows consumers to pay for purchases with funds stored on plastic smart cards. Visa, Citibank, Microsoft, Digicash and CyberCash, Inc., are all developing electronic money schemes for use on Internet or in smart card form.
* Electronic Share Information, Ltd., is seeking a license from Britain's Securities and Investments board to start the first British stock exchange on the Internet.
* Debit card transactions will permit person-to-person cash payments on the Internet.
* All of the transactions listed above operate in an environment where identities are often concealed. National borders do not exist and transactions are instantaneous and potentially untraceable.

http://www.subcontinent.com/sapra/bulletin/96feb-mar/si960308.html
Cont.

- Online pornography & adult movie
- Online matchmaking business
- Online sex or dating service
- Online consulting firms
- Online education, lectures,...
- Online payment, gift cards (WalMart & Sam’s club skim)
- Online auctions and various retail shops operating in cyberspace
Cont.

- Online underground banking system
- When age-old hawalla meets the 21st century cyber-tools
- Anything can be possible?
Cyber money-wash in Korea

- It’s the dawn of the nightmare?
- Purchase of cyber money in online game-site
- Game-money of online-game
- Mobile banking through cellar phone (phone number is equivalent to account number!!!) (e.g. Nemo service through SK telecom)
- Online gambling (casino, horseracing, sports betting) - in this case, website can be legitimately operating in offshore
Cont.

- What can be expected more!
- Cyber consulting
- Online shopping mall
- Online auction
- Online advertisement
- Many others

- Combined with identity theft, hacking, cybercrime,
- In coordination with offline/online blackmail, bribe, ...
What can be done: Law enforcement

- Law-making
- Regulations
- Undercover operation
- Training & education
- Cooperation with other countries
- Cooperation with civilian entities & private individuals