Countering Cybercrime through Money Laundering Regimes

Ann Mulligan & Sonal Dashani

What is Cybercrime?

- Definition depends on the purpose of using the term

- Dictionary definition is

“Criminal activity or a crime that involves the Internet, a computer system or computer technology; identity theft, phishing and other kinds of cyber crime”

The Budapest Convention

The Budapest Convention has an inordinately long definition of cybercrime as it seeks to identify the various types of cybercrime but it may be more helpful to identify the four categories of cybercrime offences:

i. Cyberfraud for gaining illegal possession of funds

ii. Cyberfraud for gaining illegal possession of information

iii. Interference with the operation of information systems for accessing management information systems

iv. Other offences

How much of a problem is Cybercrime?

- Cybercrime is a global plague
- New and evolving technologies provide almost complete anonymity to criminals seeking to exploit this arena.
- 40% of the world population (2.5 billion) use the internet
- Forecast that another 1.5 billion people will get access to the internet over the next four years.
- The number of connected devices will almost triple by 2020 from 13.4 billion to 38.5 billion
- Global losses inflicted by cybercrime exceeds **US$100 Billion**

Why is cybercrime so difficult to detect?

- Cybercrime can be committed from anywhere in the world
- Relatively easy and cost effective crime. All you need is a computer and access to the Internet
- Difficult to trace identities
- There are criminal organisations that exist whose sole job is to commit cyber offences – Hacktivists
- Those who are the victims of cybercrime do not always want to disclose the fact to investigating authorities

Main types of Cybercrime

- Unauthorised removal of funds from bank accounts
- Payments card fraud
- Distribution of computer viruses
- DDoS attacks against websites
- Use of Malware

What is money laundering?

Money laundering is the process by which criminal proceeds are sanitised or ‘cleaned’ to disguise their illicit and unlawful origins.

In order to fight against this there exists:

- The Financial Action Task Force on Money Laundering (FATF)
- Framework of Anti Money Laundering (AML) measures covering the Criminal Justice System and the financial sector
- Money laundering and Proceeds of Crime Legislation introduced to the Caribbean

Cybercrime and Money Laundering

- Unlike ‘traditional’ money laundering methods which rely on the banking system, cyber-laundering depends on the use of various types of transactions ranging from wire transfers, cash deposits/withdrawals to money mules.
- Use of accounts opened with lost documents or nominees
- Use of fictitious companies
- Use of cash in the final stage of the chain
- Conversion of stolen funds into cash/cash withdrawals via ATM

Money Laundering Legislation in the Caribbean

- Antigua – Money Laundering Prevention Act 1996
- Barbados – Money Laundering and Financing of Terrorism (Prevention & Control) Act 2011
- Belize – Money Laundering and Terrorism (Prevention) Act 2008
- Dominica – Money Laundering Prevention Act 2011
- Grenada – Proceeds of Crime Act 2012

- Guyana – Anti Money laundering and Countering the Financing of Terrorism Act 2009
- Haiti – Laundering Act of Assets coming from the Illicit Traffic in Drugs & Other Offences
- St Lucia – Money Laundering Prevention Act 2010
- St Vincent and the Grenadines – Proceeds of Crime Act 2013
- Trinidad & Tobago – Proceeds of Crime Act 2000

What does the legislation do?

- Provides for the requirement of persons acting in the course of business to conduct customer due diligence
- Provides for Anti Money laundering (AML) regulations
- Provides offences for failing to report suspected money laundering
- Provides Regulations that apply to persons acting in the course of businesses

Bangladesh Bank

- The ultimate cyber heist of modern times
- Dozens of fraudulent transfers seemingly executed by the Bangladesh Bank to the value of $101m
- Had some of the transfers not been queried, the value of the fraud would have been $951m
- Involved end accounts in the Philippines
- Purportedly for Bangladeshi infrastructure projects including bridges and a power station
- Money ultimately disappeared into the casino industry – yet to be recovered.

What went wrong?

- Investigators trying to follow the money lost the trail in the casinos
- A lack of procedures meant that no-one had identified the fraudulent transfers for over 2 days
- This involved transactions concerning the New York Fed who blocked 30 out of 35 (Swift) transactions.
- Malware likely to have been planted in the computer system a year previously.
- No procedures in place nor common understanding between Bangladesh Bank and New York Fed which may have otherwise alerted someone to the problem

What is being done globally to prevent cybercrime?

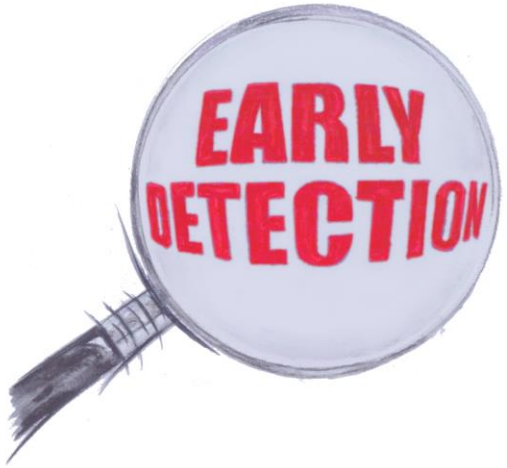
- The Budapest Convention on Cybercrime 2001 was the first international treaty on crimes committed via the internet and other computer networks by seeking to harmonise national laws. Drafted by the Council of Europe but is open for ratification by non members. The US signed it in 2007.
- FAFT has the primary responsibility for developing a worldwide standard for AML and CFT
- Global project on cybercrime launched by the Council of Europe
- European Cybercrime Centre (EC3) attached to Europol

How can AML regimes be used?

AML regimes provide their jurisdictions with useful tools for:

- Detection
- Investigation
- Cooperation
- Confiscation

Detection

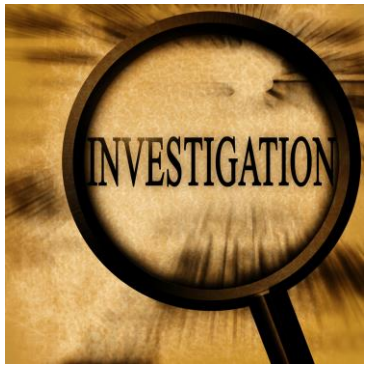


The use of Financial Investigative officers

- An under-used resource
- Invaluable
- They have the ability to apply for bank information – help to identify
- They can restrain
- Identification of financial transactions suspected to be linked to laundering cybercrime proceeds
- Strengthen responsibility of service providers to ensure they monitor the use of their services (with regulatory support)

Develop an Investigation plan

- Gather material to support a stand alone money laundering charge
- Look for evidence of origins of criminal property including circumstantial evidence, forensic evidence and use of audit trails
- Use Proceeds of Crime Act to obtain information about bank accounts to identify any large unexplained sums of money
- use search powers to search home address of suspect to help identify evidence of unexpected wealth and/or luxury items
- Consider restraint proceedings early on
- Use surveillance



Investigation continued

- Data sharing
- Ensuring all relevant offences are being pursued –think outside the box
- Requiring private organisations to reveal when they have been the subject of cybercrime
- Use powers to suspend bank accounts
- Ensuring a specialist cybercrime investigation unit exists
- Use powers to interview suspects to get them to explain movement of funds

Cooperation

- Ensuring cooperation between the private sector and law enforcement agencies
- Ensure persons acting in the course of business are aware of their responsibilities. This includes: Lawyers, Accountants, Estate agents, Trust or Company service providers, financial institutions
- Information sharing
- Use of national and international databases

Confiscation

- One of the most valuable tools in the fight against cybercrime
- Confiscation powers mean that the cybercrime trail is disrupted
- This means both a disruption to the offending and also acts as a deterrent
- Use cash seizure powers
- Use forfeiture
- Ensure confiscation is pursued in every major and organised crime

How to use ML regulations?

1. Identify as clearly as possible the suspected benefit from criminal conduct (‘the criminal property’)
2. Identify the reason(s) for suspecting the property is criminal property
3. Identify the prohibited act/s you seek to undertake involving the criminal property
4. Identify any other party/parties involved in dealing with the criminal property

Suspicious Activity Reports regime (SARs)

- Having an effective SARs regime is essential to combatting money laundering
- SARs are potentially a critical intelligence resource and provides a good opportunity for law enforcement agencies to intervene and disrupt money laundering
- Ensure that there is continued training

Summary of what needs to be done

- Ensuring properly trained AML compliance officers
- Linking AML and cybercrime units
- Creating mutually used databases
- Cross training AML compliance officers to be cyber-AML professionals
- Coordinated training of security industry and AML professionals
- Better use of FIUs

Other initiatives

- Joint Money Laundering Intelligence Taskforce (JMLIT) –A pilot as of Feb 2015 to establish better cooperation between public and private sectors on illicit finances.

- This has been found to have enhanced collective AML detection capability

- The creation of international Liaison officer posts - International cooperation is essential.

Questions?