Mr. Tony Kwok Man-wai
Former Deputy Commissioner, Independent Commission Against Corruption
The Hong Kong Special Administrative Region of China

Introduction

Firstly, I wish to declare that I will be speaking in my capacity as an individual expert, not a representative of Hong Kong. I am an expert on corruption, having served in the Hong Kong Independent Commission Against Corruption (HK ICAC) for 27 years. In HK ICAC, we dealt with not only corruption but also all corruption related crime, including economic crime. Based on the hypothetical case, I have the following observations and comments.

- In the investigation of economic crime, one should not overlook the possibility of corrupt involvement in the hypothetical case, it is highly likely that corruption may be involved in the following scenario:

  - There might be a corrupt relationship between Mr. Alan & Mr. Banner. It would be inconceivable that Mr. Alan had abused his position purely due to friendship, without obtaining some sort of advantage from Mr. Banner.

  - Lawyer/accountant accepted an advantage from Ms. Chung in setting up the shell company.

  - Instead of retrieving bank data from rubbish bins (which is rather unlikely these days), bank staff might accept an advantage in divulging a client's information.

  - Bank staff of Goldfingers Bank accepted an advantage in assisting Ms. Chung to open the account.

  - Mr Alan accepted an advantage from Ms. Chung for giving a false bank assurance.

  Hence one must also investigate all the possible corruption. If we want to be effective in tackling economic crime, we must ensure that private sector corruption is a criminal offence.

- Secondly we should spread our investigation net wider to cover other possible offences. On the breach of trust in regard to the loan, there is also a possible offence of bank fraud, i.e. the bank has been deceived by its own staff and client in awarding the loan. The investigation will entail meticulous examination of bank documents.

- In Hong Kong, we had lots of criminal prosecutions of such cases. Apart from the typical offences of conspiracy to defraud and deception, we can also prosecute offenders for false accounting and forgery. It is also an offence when an agent (employee) uses a false document to deceive his principal. Hence in this case, if it can be proved that the bank manager had made any false representation in any documents in the loan transaction, he will be guilty of the offence.

- The prerequisite to effective investigation is the setting up of a user-friendly public complaint system, so that the offence can be discovered at an early stage. In the hypothetical case, it is doubtful whether any members of the public who might have suspicions of the scheme, knew the channels for lodging a complaint. The country designated law enforcement agency must ensure there is sufficient publicity of the complaint channel. One way is to establish a cyber police station.

- Proactive Investigation – There are often two methods of investigation. One is the reactive type, after the offence has been committed - this is very difficult. The ideal is the proactive method. If we came to be aware of the scheme early enough, one can use a telephone intercept and undercover agents for entrapment. In such a case there is a good chance to get all the culprits and the mastermind red-handed.

- There is a need to encourage use of undercover agents operating in cross jurisdiction. Also sharing of undercover agents. The HK ICAC had a case of getting the assistance of an overseas law enforcement officer to act as an undercover officer in HK. It would be useful to identify best practice procedure in the use of undercover agents.

- On the Consumer fraud case, there are several difficult aspects to the investigation – cyber crime, identity theft, computer forensic, extraterritorial.

- Information Technology can be a threat and aid to investigation. As a threat, it makes the criminal activities more sophisticated and transnational; As an aid, it can assist in intelligence analysis, behavioural profiling, as a crime prevention/detection tool using data mining (process of discovering unknown patterns and relationships amongst variables by analyzing data from different sources with statistical and pattern cognition techniques) and complicated financial investigations.

- Compared with physical evidence, the advantage of digital evidence is that it can be recovered even after deletion/destruction, given the right forensic tools (and this is unknown to most criminals). The problem is the process of collection, recovery of data, authentication, analysis and how to ensure the integrity of the evidence.

The issues here are:
  - Capability of law enforcement agency in computer forensics
  - Encryption and passwords
  - Proper training of all investigators in the seizure and collection of evidence, to ensure integrity of evidence
  - The authentication of expert evidence in court
  - Transnational problems – different laws and co-operation

The solutions are:
  - Sharing of forensic expertise
  - Training centre for investigators - UNAFEI
  - Recognized scheme of experts
  - Legal power to law enforcement agencies in obtaining passwords
  - Intercept – fax, email, SMS

- On the collection of evidence from internet service providers, firstly, all countries should have a licensing requirement for ISPs. Then, there is a need for legal provisions to ensure the co-operation of the Internet Service Provider; power to require production of records, to keep log files for an extended period (90 days); and legal access to encryption and passwords, etc.

- International cooperation – At present there are provisions for judicial assistance (Letter of Request system) and mutual legal assistance. However, both normally require availability of evidence to trigger off the assistance. This is not good enough. There is a need to develop closer mutual investigative assistance amongst agencies – including assistance in bank a/c checks, telephone interception, surveillance, joint search operations, undercover operations, and sharing of evidence.

- There should be adequate legislation to facilitate investigation, to cover

  - definition of the full range of possible offences –conspiracy, attempt, fraud, deception, false accounting, forgery and private sector corruption

  - provision of adequate investigative powers – bank a/c, telephone interception.

- Capability to conduct financial investigation and on money trail, so as to obtain the evidence; recover the money and make it difficult for the culprits to get their ill-gotten gains. Use of forensic accountants.

- Use of immunity witness – Hong Kong has a resident informant scheme, where the accomplice has to plead guilty to the offence first before becoming an immunity witness. In return, he is entitled to have 2/3 of his normal sentence reduced and he is subject to protection whilst in jail custody as well as after his prison sentence.

- Intelligence support – no criminal investigation can be successful without intelligence support. Agencies should be prepared to share intelligence on cyber crime.

Building Integrity in Financial Institutions

- HK ICAC is one of the few anti-corruption agencies that are actively involved in building integrity both in the public and private sector, and have 30 years of experience in both.

- Hong Kong has effective legislation against private sector corruption.

- HK ICAC has dealt with many major corruption related bank fraud cases in the past. Just to take two examples:

    - The Overseas Trust Bank Case – this was the third largest local bank in Hong Kong, which collapsed in 1986 due to loss in bad loans amounting to US$385M. I was head of a joint ICAC/Police Task Force set up to investigate the collapse. This investigation revealed numerous incidences of bank fraud and corruption involving senior management of the bank. As a result, there were five major successful convictions, including the chairman, managing director, the general manager of the bank and the fraudster.

    - Bumiputra Malaysia Finance case – this was a case of the proprietor of a publicly listed company bribing senior bank officials to obtain massive loan and credit facilities. In the end, the listed company collapsed and the bad debt to the bank amounted to US$850M. The investigation and prosecution took 15 years to complete, with successful extradition and prosecution of the bank's chairman and two directors, and of course the listed company proprietor. The bank's internal auditor was murdered just prior to the investigation and the legal advisor committed suicide.

- HK ICAC has been assisting the banking sector in integrity building through the three pronged strategy – prevention (system control, procedural guidelines, supervisory checks, transparency and accountability), education (staff integrity, code of conduct), and deterrence.

- Zero tolerance & a proactive policy versus don't wash your dirty linen.

- ICAC offers advice to enhance the system and audit control in the bank; and in partnership with the Association of Bankers, issue best practices packages.

- ICAC, supported by business associations, set up an Ethics Development Centre. It serves as a resource centre as well as an advisory service to assist banks to draw up their unique code of ethics. ICAC recommends that the code should cover, amongst other things:

    - Restriction on staff receiving gifts and lavish entertainment from customers

    - Requirement for staff to declare their private investments and any conflict of interests

    - Strict prohibition on unauthorized disclosure of confidential or restricted information

    - Clearly stipulate the relationship between bank staff and customers.

- ICAC publish a "Practical guide to bank manager".

- I have been advocating that banks should consider having an "Ethics manager" within the financial institution, responsible for:

    - Formulating an effective internal anti-corruption/fraud strategy

    - Adopting a 3 pronged strategy –– i.e. system prevention, ethics building and deterrence

    - Setting up and administering an internal complaint system – an effective complaint system should include:
        - Encouraging complaints
        - Promising confidentiality
        - Protection of whistle-blowers
        - Quick response capability
        - Professional handling/investigation
        - Accountability to complainant and suspects

    - Staff monitoring and conducting internal investigations

- Look for red flags
  - Big spenders
  - Staff with financial problems
  - Rule breakers

  And prompt investigation

- Partnership with law enforcement agencies, instead of adopting a "don't wash your dirty linen in public" policy!

- Universities should be encouraged to organize diploma/certificate courses on ethics management. I have set up the world's first Postgraduate Certificate Course at the University of Hong Kong to provide training for such positions as well as for anti-corruption officials.

Conclusion

I suggest the workshop can seek to have agreement on the following future actions, in addition to recommendations from other panellists, for inclusion in the Bangkok Declaration:

- Each country must have comprehensive legislation criminalizing private sector corruption, with a dedicated agency responsible for law enforcement

- Setting up a centralized training course for cyber crime investigators

- Promoting the establishment of an "Ethical Manager" in banks, to demonstrate that the private sector has a clear role in fighting corruption in society

- Simplifying the procedure for mutual legal assistance and enhancing inter-agencies mutual investigative assistance

- Prepare model legislation to enforce cyber crime

- Establish an expert research centre for computer forensics

- Establish a centralized intelligence databank on economic crime and money laundering.