

IN THE BACKGROUND

December/January 2003

In this issue:

- ❖ Corporate Fraud
- ❖ Due Diligence
- ❖ The USA PATRIOT Act

Corporate Fraud – The Basics

I often read statements from a partner of an accounting firm or a representative of one of the accounting industry bodies saying that fraud is not something that can be predicted. That anybody determined enough will be able to break into, and rip off a system.

This is not true!

In every fraud that I have investigated over the years I have always seen a business control that failed, a warning sign unheeded, a missed opportunity for minimising the exposure.

Over the next few editions of In the Background, I am going to try and set out some of the steps a business can take to insulate itself against fraud and also to explain the different things that you can do if you are the victim of a fraud to mitigate the amount you lose.

In this edition I deal with the basics of what a fraud is, what types of fraud there are and what are the essential things that you need to do to protect against fraud.

What is Fraud

Fraud is simply theft with deception. Around Asia fraud is treated differently in each respective jurisdiction. In some countries they have an offence of fraud, in others they have a number of offences under theft legislation or a proscriptive crimes act.

Fraud is also a term used to generically describe various offences involving self-dealing or corruption. This is appropriate as many of the same procedures to insulate a firm against theft can also be used to protect it from other forms of corporate abuse.

For each jurisdiction that you are involved in you should get some basic understanding of the key commercial crime legislation. Your law firm can help you here.

Knowing what the local authorities say is a fraud will help you evaluate the seriousness of any instances of potential malfeasance.

Another important starting point is to look at what your corporate compliance manual deems unacceptable behaviour and to compare that to local laws. I have seen instances of forging documents that were technically not a fraud in Korea and Japan, and instances of bribery and self-dealing that did not breach any law in some countries in the region. When the law is inadequate you should ensure your internal policies prescribe what is acceptable. Likewise you need to ensure that the manual ties in with the laws and is blunt about what is not acceptable.

In a later article I will cover some of the key control issues that firms need to consider and in this respect, understanding the environment you operate in is an obvious one. Understanding the legal framework is part of this.

A common misconception is that frauds are sophisticated or complex. I sometimes read articles that portray the fraudster as some kind of wicked genius. Again most of the time this is just not true. Fraudsters are just thieves and most of the time are motivated by greed. Most frauds are reasonably simple to understand.

In any fraud there are three key elements – planning, execution and concealment. I discuss below three basic types of corporate fraud and how planning, execution and concealment is different for each.

Why Worry

Fraud is one of the few things that can destroy an otherwise functioning business very quickly. We have found that total losses from a fraud when you add up the actual amount taken, lost business, lost reputation, increased compliance costs and the costs of the investigation itself are in region of at least three times, and more likely five times, the amount actually stolen.

As well as financial costs there are often considerable human costs as firms and regulators seek to place blame on those that let this happen on their watch.

Not only can you protect against fraud but also you must do it.

In every fraud that I have investigated over the years I have always seen a business control that failed, a warning sign unheeded, a missed opportunity for minimizing the exposure.

The Three Types of Fraud

There are really only three types of corporate fraud. Each type requires a different strategy to perpetrate and different types of controls to prevent.

1. Employee Fraud

This is the most common type of fraud, where one or more employees of a firm conspire to steal from it. These types of frauds tend to be of low value in each specific event but can add up to considerable amounts.

What distinguishes employee fraud is the narrowness of the fraudulent activity. The fraud takes place in the area of influence that the employees have. The more employees and departments involved the further the fraud spreads and vice versa.

Employee fraud normally involves some planning in terms of the employee figuring out which of the business controls that they interact with that they can subvert and there is sometimes a test run to see how the control environment responds to an isolated attempt.

Another interesting characteristic of serious employee fraud is that the employee was often disciplined some months before the major fraud is discovered for a minor transgression.

The fact that many major frauds come from effectively repeat offenders lends support to our view at [BACKGROUND ASIA](#) that firms should adopt a zero tolerance policy where they have a clear case of employee fraud no matter what the dollar sum involved.

The execution of an employee fraud almost always happens when the employee is there.

The often cited audit control of enforcing annual leave is one easy way to make employee fraud just that little bit more difficult. Of course some employees know this and work with other employees who cover for them.

Some years ago I investigated a fraud that took place over five years and was perpetrated by just two employees who never took leave at the same time and were therefore able to cover for each other.

It is worth noting here that it is easy to recommend these types of controls but sometimes they are very difficult to implement in practice. The key is to recognise the control weakness and to alter other policies and controls to allow for this. If it is impossible to enforce a strong leave policy then maybe that part of the business should get a little more internal audit attention than another part that can implement a strong policy.

Concealment is a very important element of employee fraud. Most employees only steal amounts to top up their income. Sometimes it is to fund a specific loss like a gambling debt or stock market loss. Most of the time they want to keep their jobs so once they have perpetrated a fraud they then do what they can to conceal their actions.

I have not seen many employee frauds where the amount stolen in one act is very large. In cases where the amount taken in one act is very large then the employee will typically breach so many controls in executing the fraud that you could compare their actions to that of a management fraud, discussed below.

Employee fraud is therefore best addressed by looking at how easy it is to conceal a fraud involving that employee. For example if nobody ever checks the guy that signs off on stock obsolescence then he will be easily able to conceal his own pilfering.

Two key things to think about when evaluating controls in this respect are: What is the dollar value of any one single act that would not normally be subject to any form of review; and what is the dollar value of any series of acts that would also not be subject to review.

When considering frauds involving employees conspiring together you need to extend this analysis of amount and frequency to incorporate both employees.

It is rare than an employee fraud will destroy a business but there are examples of it. Nick Leeson is probably the most infamous and each year you will read about rogue employees who do bring a business down.

2. Management Fraud

This is less common and more difficult to detect. It is also much more dangerous than employee fraud as management are often able to override controls put in place to detect fraud and then cover up their activity.

Management frauds tend to be much larger than employee frauds but less frequent in number.

I have seen a lot of management frauds involving debtors, as a firm's sales function is often easy to corrupt. For example a senior manager tells his staff that one customer is so important that only he can deal with them.

Sometimes the customer is entirely fraudulent, and then the manager just writes off the debt.

I have also seen managers set up firms they control as customers of their company and then take a margin on the trade by giving themselves discounts and generous credit accommodation.

The only good thing about frauds involving debtors is that they do not often destroy businesses.

Another common management fraud involves large transactions for overvalue. The manager gets his firm to execute a large transaction that benefits him and the transaction is poisoned with non-performing or non-productive assets, which can destroy a company.

Enron is the best current example of a management fraud that destroyed a business. The insertion of the off balance sheet partnerships where senior management was extracting large payments and fees caused the crisis of confidence that obliterated the firm.

3. External Fraud

This is the least common fraud but still one that affects many businesses and individuals in Asia every year.

External frauds are when an external party or group attacks a business.

External fraudsters sometimes corruptly induce or extort an employee to assist them and this possibility should be not be ignored when looking at external frauds.

External frauds involve quite a bit of planning. Generally the external fraudster (unless it is a former employee – another common occurrence) does not understand the business control environment and so will execute a number of attempts at the fraud to test the system. The test run will normally be for a very small dollar sum so as not to alert a company to the control weakness if it works and so as not to get caught if it doesn't.

Once the fraud has been planned the external fraudster then looks to execute the fraud.

A key point about an external fraud is that the fraudster expects that the fraud will be discovered. They do not prioritise concealment and therefore they will look for one big attack on a business with a view to putting as much time between the fraud and the event that they can, without worrying too much about a sophisticated concealment. This should be contrasted with an employee fraud that generally does involve concealment.

A common ploy is to execute these types of frauds around the time of public holidays, thus giving the fraudster one or two extra days to cover their tracks after the fraud.

The concealment that they will do is in concealing where the money actually went. Normally this is done by laundering the funds through multiple accounts, cashing those funds out of accounts and then placing them in further accounts sometimes after walking the cash across nearby borders.

In investigating an external fraud you need to focus on the precise nature of the events that lead to the theft-taking place and in trying to trace the funds as best you can. It is often in carefully reviewing these facts that you find a slip up which will lead you to one of the perpetrators or an internal accomplice.

There are frequently reports of different gangs perpetrating frauds in the region. Advance fee frauds, LC scams, fake stock scams, funny money scams are still commonplace. There is also a rising concern amongst some law enforcement officials that organised crime gangs are moving more into fraud, and in particular, high tech fraud. The money, the low conviction rates and the low sentences upon conviction are attracting these gangs away from traditional organised crime businesses like drugs, prostitution and extortion.

Firms that think they are the victims of an external fraud need to respond very quickly. Every day is critical after the money has gone if you are to have any chance of getting restitution or even arresting the fraudster.

How to Protect Against Fraud

There are actually only four things you need to do to protect your business against fraud. The good news is that if you get the correct mix of these four things then they work together to insulate the business. The bad news is that they aren't that easy to implement effectively in Asia and require continual vigilance and review.

All frauds can be prevented by:

- 1. Engaging Honest Employees;**
- 2. Having Strong and Relevant Internal Controls**
- 3. Ensuring Firm Enforcement of Policies; and**
- 4. Understanding asset security.**

As I said earlier, these seem simple but in fact there is a lot to them.

Employees need to be screened and carefully considered for the role that is envisaged for them. They need to be periodically evaluated. Management needs to look at whether their personal circumstances are consistent with what they earn. Get to know those employees in key positions of trust better than you normally would. I've never seen an investment in any of these aspects of employee management not paying off.

Internal controls need to be strong, but most importantly relevant. Controls need to take into account the environment that you operate in. Controls that work well in Southern California don't necessarily work well in Malaysia.

In one investigation I was involved in a firm had a policy of asking employees to make their own decisions about tenderers where they specifically told employees to evaluate more than just price. A group of employees who then took kickbacks were able to argue that the company's policy did not mean they couldn't do so.

What seemed an obvious prohibition in the US was something, which should have been spelt out in Asia.

Companies need to have strong and consistent enforcement of their integrity programs and policies. Employees, who see such a policy in action when a fellow employee is dismissed or arrested, are less likely to engage in fraud or malfeasance themselves. Conversely employees that see staff abusing the system, particularly management, will look to get their slice of the action as well.

The companies that I have seen with the worst internal frauds have been the ones with a history of poor compliance and poor examples being set by management.

Asset security is an important part of the business controls environment. Understanding what your business assets are and what you need to do to protect them from theft is very important. Fraud is all about getting access to an asset and then getting away with it. The harder this is the more difficult a fraud will be.

I have found that some firms concentrate their control policies on typical audit controls and neglect basic asset security. In Korea you can do just about anything with a company chop. In Japan you can do a lot with a blank check. In China it is just about impossible to trace stolen goods.

When we are asked to review the business control environment we separate our review of the firm into a review of the nature and effectiveness of the four elements above.

We look at the interplay of those four elements as a weakness in one can be balanced by strength in another but the absence of one will often negate the effect of another.

In the next edition I will discuss some of the things that can alert you to a fraud and what you can do when you first discover one.

Cheers

Alex Duperouzel

alex@backgroundasia.com

DUE DILIGENCE

How much is your deal worth?



We help you understand the nature of the potential risks and opportunities in a transaction. We supplement your existing due diligence process either as part of the team or as a discrete service, separate to the team.

In this article we look set out some of the things that you should consider prior to going into a deal in Asia and some of things you can consider if a deal is not going well. The article also looks at what you can do to know your own people if you are putting them in a position of trust or responsibility.

Ric Beggs

ric@backgroundasia.com

The Deal – Do you have all the facts?

With the slow resumption to normal following the long “winter of discontent” in the aftermath of the 1997/98 Asian Crisis, some investors are tentatively seeking out potential investments, these are not those seeking trade cheap debt in the once giants of corporate Asia, but longer term strategic investors.

While there is not a stampede to buy companies at any price, there are buyers, buyers who are more discerning and thorough about potential opportunities.

There is a different mood emanating from these investors; it is one of considerable caution with strict priorities on knowing the industry they are getting into, knowing the management and understanding market and political risks.

So what should you do if the deal is due to be signed once the papers are ready. You have had endless meetings pouring over the accounts; you’ve met all the directors and believe they manage a good business and that their company is an ideal investment or joint-venture partner.

But how much do really know about the principals of the company?

- ❖ How did they come to be in this business?
- ❖ Where did they get the money to start the business?
- ❖ Do their respective spouses or relatives operate independent businesses that might depend upon the business you are about to enter?
- ❖ Is there any history of litigation, company or personal?
- ❖ Do the principals hold shares in any other undisclosed companies?
- ❖ What did they do in the last deal that they did?
- ❖ Are there any areas of potential conflict of interest?
- ❖ Are there any business or social relationships that might embarrass your organization?
- ❖ Are there any connections to organized crime, money laundering or drugs?
- ❖ Are the key staff planning to leave if you invest?

Normally, legal and accounting due diligence will not uncover the answers to these questions. In the past investors were content with industry comment and would do the deal based on a perceived reputation.

In the continuing aftermath of the 1997 Asian Crisis and in dealing with today's economic slowdown many of the as yet unpaid creditors had done just that, they relied upon hearsay reputations, perceived industry standing and what they thought were the target company's business and political connections.

In considering a transaction or a new relationship for your organisation, you will need timely and accurate intelligence to aid you in making the correct decisions. **BACKGROUND ASIA** conducts discreet pre-transaction intelligence concerning the target company(s) and its principals. The focus is on the principal's business capabilities, management experience and competency and reputation.

Pre-Transaction Intelligence

This form of discreet background checking is not designed to prevent the deal, but merely provides a means of obtaining information to enable informed opinions and decisions to be made, for risks to be mitigated, for transactions to be structured to take into account what is really going on at the company.

At **BACKGROUND ASIA** we call it "Off-Balance-Sheet" due diligence, complementing the legal and financial quantitative due diligence, digging into background of the corporation and its management, analysing track records, successes and failures, strengths and weaknesses, litigation history and international relationships, whether they are distributors, joint venture partners or investors, highlighting political, relationship, intellectual property, NGO and technology risks.

Asia is notorious for its lack of accurate, timely or even truthful public records systems. Pre-transaction intelligence focuses on the human element and what key stakeholders are saying about the target company. That intelligence is then analysed in the context of the deal and recommendations are presented to mitigate risks where that is possible.

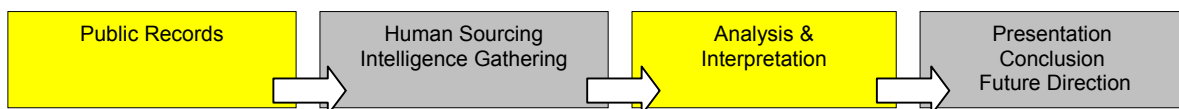
Pre-transactional research will include, but will not be limited to:

1. Corporate structure of the company (key officers, shareholders and subsidiaries).
2. Background and current activities of the subject company.
3. Reputation of the subject company in the industry (competitors, trade organizations).
4. Reputation of the subject company with its associates (suppliers and employees).
5. Current status of any other international joint ventures.

6. Activities and background of professional management of the subject company.
7. Limited financial information, as available.
8. Litigation history of subject company and key individuals.
9. Regulatory issues (Stock Exchange, Company Registry and other Government bodies).
10. Labour issues, if applicable (history and status of strikes/disputes).
11. Character, integrity and reputation of the subject individuals (owners/key officers).
12. Level of political connections of key subjects.
13. Professional and personal relationship between subject individuals.

Commercial Intelligence

Intelligence Gathering & Sourcing Process



Global and regional businesses face a wider array of challenges than they ever have. The increasing complexity of regulations, the speed of communications, the way large amounts of data can be easily collected and disseminated to a competitor and the information available to every organization through the Internet increases the risks faced by today's business manager.

Without the timely intelligence and facts there is the likelihood that you will be exposed to potential fraud, corruption or worse.

The traditional ways of doing business are changing and customers and suppliers are no longer driven by loyalty and competitors will use every available legitimate means and sometimes, illegitimate methods to gain market share.

Joint ventures often do not live up to their original promise. Was the joint venture just a bad business decision or was their something more sinister or calculating involved?

One of the essential keys to business success is timely and accurate intelligence that allows senior management the option to make informed decisions and execute a rapid response. **BACKGROUND ASIA** works behind the scenes to collect and analyse intelligence relating to a company or deal while abiding by the laws applicable to the client and the operational jurisdictions.

Typically we are involved in researching the full background of a transaction finding out what took place from those actually involved and then gathering intelligence in relation to the current issues affecting your counterparty. We then work with you or your counsel to formulate a strategy for solving the issue. Sometimes this is legal solution, sometimes it involves law enforcement, sometimes it is a commercial solution.

On the larger issues we have worked on it is normally a combination of all three.

The research conducted is a combination of public record data research (recognising the limitations of this in some locations) and discrete human intelligence sources. After research is done there is sometimes an opportunity or a need to execute a strategic operation that would involve the placement of information or the live collection of further intelligence by way of a sting or pretext.

The foundation of any form of live actions that you decide to take is always based on an appreciation of the intelligence you have and the legal implications thereof.

The USA PATRIOT Act

As a result the 2001 September 11 terrorist attacks on the United States the federal Government has passed a challenging new law imposing new regulatory requirements on financial institutions.

The law has significant extra-territorial implications for financial businesses operating in the Asian region.

Regulators in the US have told **BACKGROUND ASIA** that they intend to enforce the act's provisions aggressively and let the courts rule on contentious grey areas.

If you are in the financial business and you don't understand how the PATRIOT Act will affect your business in Asia then you should look into it. There are a number of US law firms now providing excellent advice on the applicability of the act and we recommend that you consult with your US counsel about how it might affect your business in Asia.

Why Worry?

For those non US firms wondering why they should bother complying with a piece of US legislation you need to consider the scenario under which it may touch upon you.

Say you are an investment fund and for years have had a small US charity, The Holy Land Foundation, as one of your fund investors.

Law enforcement authorities conduct an investigation using wire taps, access to bank records and various special powers of arrest and detention relating to the war on terror. They then conclude the Holy Land Foundation supports terror and blacklist it via the regulatory mechanisms that they have.

The next thing they do is knock on your door and ask you to show why you should not have known about the activities of that foundation.

They have the benefit of 20/20 hindsight, you had relied on the fact that the foundation was a registered US charity.

The publicity associated with their inquiries of you, and there will be publicity, can ruin your business. There are severe financial and criminal penalties now associated with negligence in relation to your anti-money laundering procedures – as opposed to other prior legislation which has tended to talk of actual knowledge, not what you should have known.

US prosecutors will only go after the cases that are the most serious but when they do, watch out.

Some Background

The USA Patriot Act of 2001 is an acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." The act applies to financial institution and that term is broadly defined to cover a range of financial entities, including investment companies, brokers and funds transfer operations.

The act does reach outside of US borders by specifically including some firms that transact in US dollars or have US investors. There are carve outs in relation to the act but they are limited and sometimes technical.

For example The US Treasury Department, the government department charged with enforcing this new law (see www.ustreas.gov/topics/law-enforcement), are now interpreting the term “investment company” under the Act to broadly include all forms of investment funds, including private investment funds such as hedge funds and venture capital funds, not just SEC-registered and regulated funds that fall within the definition of “investment company” under the Investment Company Act of 1940, such as mutual funds.

The act has different provisions in relation to banks, private banks and other financial institutions. However in general it could be said that it compels those organisations that it applies to to have anti-money laundering procedures and policies, to check that they are not dealing with a number of proscribed individuals or groups and to have some way of confirming that those policies and procedures are being followed.

It is also important to note that the act does not just cover firms who deal with funds relating to terrorism or drug trafficking (the original crime covered by anti-money laundering laws), but also relates to some 300 indictable offences in the US. In essence if your client is involved in processing or handling funds relating to any serious crime you could have an exposure. Some of those offences include money obtained through, or with the intent to promote, bribery of a public official, embezzlement of public funds, smuggling or export control violations, extraditable offences, unlawful importation of firearms, firearms trafficking, and computer fraud and abuse.

A useful place for learning more about what is being done globally in relation to combatting money laundering can be found at the Financial Action Task Force site (www1.oecd.org/fatf/).

BACKGROUND ASIA has a kit available for hedge funds to comply with the act and has already been working with some private banks in relation to supporting their compliance efforts. We are also able to build an outsource function or build up an internal function for your Asian operations. There are provisions for outsourcing in the act.

Special Measures for Banks regarding Jurisdictions or International Transactions of Primary Money Laundering Concern

The act is very complex in relation to the provisions for banks. One lawyer described it as “The Constitutional Lawyers Relief Fund Act”.

An example of the new special provisions can be found when looking at how banks are required to deal with other foreign banks.

The regulators feel that because some financial institutions, jurisdictions and countries are known to have critical deficiencies in their anti-money laundering detection capabilities, that special emphasis needed to be placed upon these by the U.S. Treasury Department. Their concerns may arise as a result of lax money laundering detection systems or a demonstrated unwillingness to co-operate in anti-money laundering efforts such as the NCCT's (**Non-Cooperative Countries and Territories**) as identified by the FATF.

Special measures required included:

- ❖ Additional record keeping or additional reporting requirements;
- ❖ Identification of customers of foreign financial institutions who use an inter-bank payable-through account at a US domestic financial institution; and
- ❖ Increased scrutiny and restrictions concerning opening or maintaining inter-bank correspondent or payable-through accounts.

The Treasury Department has established minimum account opening standards that financial institutions must follow to verify the identity of both foreign and domestic customers. As part of the verification, FI's must maintain records of the information used to identify the customer. As mentioned above they must also consult government issued lists of known or suspected terrorists and terrorist organizations and it is important to note that these lists change on a regular basis.

To ensure efficiency and ease of complying with these regulations, money laundering detection software should be capable of maintaining files containing NCCTs and other identified jurisdictions as well as government issued lists of terrorists and terrorist organizations and it needs to be updated regularly.

In November 2001, acting on the belief that shell banks often exist primarily to hide assets and other transactions from official scrutiny, the Treasury Department issued new interim guidelines that:

- ❖ prohibit financial institutions from providing correspondent accounts to foreign shell banks.
- ❖ require financial institutions to take reasonable steps to ensure that correspondent accounts provided to foreign banks are not being used to indirectly provide banking services to foreign shell banks.
- ❖ requires institutions that provide correspondent accounts to a foreign bank to maintain records of the foreign bank's owners and its agent (for service of process) in the United States.

In issuing the interim guidelines, which implemented provisions in the Patriot Act that became binding on December 25, 2001, the Treasury Department said it expected financial institutions to promptly terminate any correspondent and must determine whether it needs to undertake further investigation and file a SAR on any client.

To facilitate the process of obtaining needed assertions from respondents in the short time provided by the law, the Treasury issued a model form of certification that the foreign bank is not a shell itself and that it will not pass any shell business indirectly to its U.S. correspondent. The certification form also requires ownership information on the foreign bank for each owner having an interest of greater than 25%.

Note that these guidelines will be subject to change and again, legal advice is necessary. Further, the guidelines address only the prohibition against correspondent banking services for offshore shells. We note that compliance with the guidelines does not satisfy any other obligation a financial institution may have under the Act, such as the need to conduct appropriate customer due diligence.

Other parts of the act focus on special due diligence requirements for banks conducting business with offshore banks. They set out varying degrees of assessment based on the geographic location of the banks or their underlying business.

The reality that we are already seeing in this respect is that some US banks are just refusing to conduct certain types of business saying that the compliance costs and risks are just too large.

Interbank accounts can be seized

One of the more interesting parts of the act involves the procedure by which the US government can seize assets of a suspected criminal where that person conducts business with a bank that has a US dollar account with one of the US banks.

Under the Act, the Government can now seize assets from an interbank account established by a foreign bank based on the alleged wrongdoing of an individual foreign depositor without bringing a forfeiture action in the jurisdiction where the foreign bank is located.

Funds seized need not be traceable to the original deposit, leaving the foreign bank liable to the foreign depositor whose funds were placed in the interbank account.

Due to similarities in the definitions of “interbank account” and “correspondent account” under Title III, correspondent accounts are expected to fall under the reach of these new forfeiture provisions.

Before the passage of the PATRIOT Act, the government was generally prohibited from seizing suspect funds from a correspondent bank account based upon the wrongdoing of a particular depositor.

However, Section 319, states that if funds are deposited into a foreign bank that has an interbank account with a financial institution in the U.S., those funds shall be deemed to have been deposited into the interbank account, and any restraining order, seizure warrant, or arrest warrant regarding the funds may be served on the US financial institution.

Funds in the interbank account may be seized to the value of the original deposit into the foreign bank without the government needing to bring a forfeiture action in the jurisdiction where the foreign bank is located.

It need not find evidence that the funds in the interbank account are traceable to the funds originally deposited into the foreign bank or that the financial institution holding the interbank account was involved in the predicate offence for the forfeiture.

One US prosecutor told us that in their view the offshore bank would have to deal with the issue of freezing the underlying client account to recover their losses if the interbank account funds were seized. The prosecutor added that the offshore bank could not be a party to any action challenging the forfeiture as the underlying client had to turn up in the US to defend the issue.

While we recognise that a number of defence counsel may not share this view we do expect battles in court over these issues and banking clients should be doing what they can to prevent themselves from getting into this sort of fight.

What Asian financial institutions should do in compliance of these new laws is again something that legal advice needs to be sought on. There are also a number of resources that can be found on the net that will help in explaining the effect of different parts of the act generally.

Private Banks

A whole section of the act applies to Private Banks. Private Banks will be required to implement policies, procedures and controls reasonably designed to detect and report money laundering through correspondent accounts and private banking accounts, and to ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, any such account.

[A private banking account is defined as:](#)

An account (or any combination of accounts) that -

- ❖ Require a minimum aggregate deposit of funds or other assets of not less than \$1,000,000;
- ❖ Is established on behalf of 1 or more individuals who have a direct or beneficial ownership interest in the account; and
- ❖ Is assigned to, or is administered or managed by, in whole or in part, an officer, an employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

PEP – Politically Exposed Persons A senior foreign political figure or any immediate family member or close associate of a senior foreign political figure.

FI's will also be required to conduct enhanced scrutiny of any such account that is requested or maintained by, or on behalf of, PEP (a senior foreign political figure), or any immediate family member or close associate of a senior foreign political figure, in order to guard against money laundering or other suspicious activity. Private banks are often faced with these situations.

We note that there is a database available for banks that purports to list a very large number of politicians and their relatives but that access to this database is very expensive.

BACKGROUND ASIA looked into the costs of securing access to this database but concluded that it would be more cost effective for clients to conduct traditional due diligence on the potential client to address the concerns of the PATRIOT Act than it would be to subscribe to the database.

Summary

In summary the provisions of the USA PATRIOT Act are complex and ground breaking in terms of their extraterritorial reach.

All financial institutions and firms operating in Asia need to understand how the act affects them. It is likely that the act does have a direct effect on every financial firm that does business in US dollars.

There are ways to mitigate the risks of the act by implementing new compliance procedures and tightening old ones.

BACKGROUND ASIA

"Strategic Solutions to Solve Commercial Issues"

www.backgroundasia.com

Alex Duperouzel: (65) 9117 3450 / (852) 91816917

Ricardo Beggs: (65) 9633 8489 / (61) 418 545 785

alex@backgroundasia.com

ric@backgroundasia.com

Notice: The content of this publication is general in nature and, as we are not a law firm, it is not intended as legal advice related to individual situations. Your law firm should be consulted for specific legal issues.

Copyright © 2002 All rights reserved. No part of this publication may be reproduced in whole, or in part, without the express written consent of the Background Asia Limited.