3rd National Anti-Money Laundering Conference

Prosecuting Money Laundering Crimes

9 November 2011
Holiday Inn, Suva

TOPIC: **Why financial institutions are at the forefront in fight against ML**

Speaker: **Mr. Norman Wilson**

Position: **Chairman**

Organisation: **Association of Banks in Fiji (ABIF)**

Prosecuting Money Laundering Crimes – Building a Strong Partnership
Norman Wilson, President Association of Banks in Fiji

AML Conference, Holiday Inn, Suva
Wednesday, 9 November 2011

Speaking Prompts

Opening remarks

- Thank you to the organisers for giving me the opportunity to speak at this year's National Anti-Money Laundering conference.
- I'd like to open with a quote from the Kroll Global Fraud Report – "If fraud were a virus, almost everyone would be slightly ill."
- However, when you consider that fraud is merely one category of several under the broader umbrella of financial crime – albeit a significant one – I think we can safely say that the financial services industry is not looking in the prime of health when it comes to being a target of these crimes.
- I don't need to tell this audience that financial crime comes in many shapes and sizes – and between us, we've seen it all - sanctions, compliance issues, conflicts of interest, corruption and bribery, money laundering, cyber crime, terrorist activity, travel, ATM, credit cards, forged documents, identity theft – the list goes on…
- The finance business is based on trust and customers trust us to keep their information safe and our reputation and 'social licence to do business' is based on this premise.
- As a customer centric industry we take this obligation seriously and aim to provide the most stringent security protection for them.

- We need to think global – whether we like it or not, we are part of a global society and we face the same risks as other parts of the globe do and we need to be prepared.

The Risks – what keeps us up at night?

- Cyber crime is on the increase and regularly makes the headlines.
- Loss of customer data - physically transferring unencrypted data carries a high risk of data loss. In fact, theft of information and data is approaching epidemic proportions and the financial services industry is right in the spotlight. In 2010, 42% of financial services organisations reported information theft, loss or attack – up from 24% in 2009 - and more than any other industry. *<source: Kroll Global Fraud Report>*

Loss of customer data - HMRC & NHS

HMRC

In 2007 the British HM Revenue & Customs department (HMRC) lost an unencrypted CD containing personal details of 25m UK citizens, including date of birth, addresses, National health numbers etc. The Head of HMRC resigned and Alistair Darling (his boss) was left to address the House of Commons and explain what went wrong.

Impact: Reputational damage, customer confidence, cost of clean-up > £150m

NHS

In 2010 a UK National Health Service employee lost a USB containing data pertaining to UK citizen's health – USB found by a member of the public and handed to the press.

Impact: Press coverage, reputational damage, regulatory investigation and remediation

- Identity Theft can destroy lives.

Identity Theft – Passport theft and murder of Hamas commander

In 2010 three stolen Australian passports were used by suspected assassins to travel to Dubai and murder a Hamas commander.

Impact: Reputational damage, legal and political issues.

- Website attacks – Financial institutions are a frequent target for hackers and organised crime.

Website Attacks – RBS WorldPay website

December 2008 details of 1.5m credit cards and 1.1m personal individual details were stolen from RBS WORLDPAY website via a flaw in their on-line portal.

Impact: Huge financial losses - $9m stolen in thirty mins. Millions of credit cards required to be re-issued. Legal action, reputational damage – Class action lawsuit – legal costs

Sony Playstation breach

May 2011 Sony executives bowed in apology for a security breach in the company's PlayStation Network that caused the loss of personal data of some 77 million accounts on the online service.

Impacts are pretty much the same as RBS WorldPay example. Sony breach extended further than just C/Card details in that customer personal information, dates of birth etc. were compromised and added another layer of risk associated with the

possibility that identity details of Sony's clients could be used to access banking and other facilities outside of the Sony environment.

- User access – As staff members move within an organisation they may aggregate different levels of system access, potentially enabling fraudulent transactions.

Inappropriate User Access – Societe Generale

In 2010 SOC Gen. Rogue Trader, Jerome Kervial abuses privileges to trade $49Bn without authorisation and then hide losses. Kervial started in compliance and moved to front office, his system access was never revoked.

Impact: SOC Gen lost £700m at time of event with further losses incurred. 6% drop on European stock markets, emergency cut in US Federal Reserve Rates.

- Social engineering such as phishing. Often a key technique in conducting online fraud.

Phishing – Bank of China

In early 2011 Bank of China (BOC) customers lost money by disclosing their details on fake BOC websites. Fraudsters then used this information to steal money.

Victims who sought compensation from the Bank of China claiming negligence on the part of the bank have not been successful as a banker said that the bank's website met the regulator's security requirements.

Impact: Financial impact – loss of customer funds estimated to be between 40 million yuan and 100 million Chinese yuan (US$6.08m-US$15.2m), Reputational damage.

- Emerging markets come with their own set of increased risks – corruption, information theft, fraud, sanctions and terrorism and of course political instability which impacts international markets, the price of oil, free trade, etc. Some of this can be deemed as state sponsored and the systemic threats we face. Imagine what havoc organised criminal institutions could create for our institutions and banks through cyber attacks.
- In fact, research has shown that these cross border risks are considered by a vast number of organisations to be a deterrent to expanding into other markets.
- The risk impacts are considerable and we have a responsibility to apply our high standards of protection to all our customers, regardless of location, even if this could put us in an anti-competitive position in some geographies. As I said, we take our responsibilities seriously.
- All this leads to the biggest risk of all – reputational risk and the damage this causes – in extreme cases this can lead to a complete erosion of confidence, a bank run or a bank closing or failing (Rigg's National Bank in Washington DC and of course, Barings, courtesy of Nick Leeson in Singapore)

Are we ready? Collaboration will be key.

- But we have to ask ourselves if we are ready for this? All the indicators tell us that financial crime is only set to increase. Combine this with our rapid growth and expansion agenda and the risks multiply significantly.
- Now is the time to get on the front foot.
- Banks are good at being reactive. Like a SWAT team, give us a 'situation' and we'll go in and sort it out.

- What we're not so good at is taking the preventative medicine. So, what's holding us back?
- The answer is clear – it's our culture of silos, it's also a mindset of collaboration and thinking in a customer-centric manner.
- We have to get better at taking a proactive approach to sharing intelligence across financial institutions, divisions and business units. Collaboration is key.
- The criminal institutions or individuals that we face are opportunistic and highly intelligent. They will seek whichever environment is most open to them and there are plenty of choices, notably centres that relax their standards of security – 'friendly tax havens'. I would urge the authorities in Fiji not to follow that path.
- We must also take a collective approach to collecting intelligence – this is a case of "the whole is greater than the sum of its parts."
- This conference is a perfect example and the desired end result is to make sure everyone here understands the process for collecting and sharing intelligence and to ensure we are helping our customers by giving the right people access to the right information at the right time.
- To be relevant, intelligence must be actionable and must add value to our customer facing staff (and ultimately customers) to help them make informed decisions.
- While many different industries and groups are represented here today, I am confident we all have the same interests – working together to fight financial crime to achieve better results.
- Thank you for your time and attention.