The Voice of Private Client Compliance and Regulation

Compliancematters

from WealthBriefing

FEBRUARY 2015 VOLUME 2 № 7

PUBLISHER: Stephen Harris
EDITOR: Chris Hamblin
PRODUCTION: Jackie Bosman
ISSN: 2053-9355

PUBLISHED BY:
ClearView Financial Media Ltd
Heathman's House, 19 Heathman's Road
London, SW6 4TJ, UK

TEL: +44 (0)20 7148 0188
SUBSCRIPTIONS: +44 (0)20 7148 0188
EMAIL: info@clearviewpublishing.com
WEBSITE: www.comp-matters.com

HSBC – WHAT THE LEAKED FILES TELL US

From hitherto-unknown details about long dead scandals to tales about the 'housewives of HSBC,' the ICIJ's revelations are a treasure-trove for compliance officers and money-laundering reporting officers. Chris Hamblin of Compliance Matters picks his way through the extensive files.

Switzerland has reluctantly begun a money-laundering investigation into the behaviour of HSBC, the world-girdling banking group whose past behaviour has re-entered the public eye because of a concerted media campaign. Geneva's prosecutor general, Olivier Jornot, and its first prosecutor, Yves Bertossa, have authorised a raid on two of HSBC's offices in that city and are conducting a wide-ranging investigation that could ensnare many private individuals as well as bank employees. They are, at present, at the document-gathering stage. Meanwhile, rather late in the day, the Financial Conduct Authority in the City of London is looking into the bank's working practices because HSBC is now dominating the political agenda.

A TREASURE TROVE

The secret HSBC files that the International Consortium of Investigative Journalists has publicised are based on data originally smuggled away by an HSBC employee and handed over to the French authorities in 2008. Most client and account data in the files comes from the period 1988-2007; amounts date from 2006-07.

PEPS AND BILLIONAIRES: HSBC'S TARGET AUDIENCE

One of the latest revelations is that the Swiss bank seems to have conducted no 'extra due diligence' on Rami Makhlouf, the richest man in Syria and President Assad's cousin, despite the Financial Action Task Force's recommendation that 'politically exposed persons' of this sort require it. In 2006 Makhlouf had about $15 million spread across many accounts at the bank. At the time – and today – he was obviously part of the Syrian 'deep state,' controlling the largest telephone company in the country, along with much of its financial services and plenty of properties. Makhlouf ended up on a US sanctions list in 2008, but nobody is suggesting that HSBC was serving him by then. HSBC also serviced Drex Technologies, a company in the British Virgin Islands that Makhlouf owned, which ended up on a sanctions list in 2012.

Many high-net-worth Canadians used HSBC Switzerland to hide their undeclared assets from the taxman, according to an investigation by CBC News, the national news channel. Canadian tax authorities obtained the data in 2010; at least 264 have now confessed. *(PTO)*

INSIDE

This edition pays special attention to three themes: a flurry of new legislation to govern regulation in various IFCs; online compliance issues; and the European Union's influence over trading environments and venues

NEWS

ARTICLES

Other Canadian billionaires such as Marcel Adams, Frank Giustra and Joseph Kruger II, however, declared everything they had there.

CONFLICT OVER DIAMONDS

Some 6,500 Israelis held about $10 billion in secret bank accounts at the Geneva branch of HSBC between 1988 and 2007 - a fact that has caused a stir in the Israeli press. Linked to Israel (and to Antwerp) is a more serious revelation - HSBC's role in the activities of Erez Daleyot, a Belgian-Israeli diamond magnate who is now reportedly under investigation in Belgium for money laundering and tax evasion. In the midnoughties, he held at times as much as $35.5 million at HSBC Private Bank 'in accounts tied to shell companies in the British Virgin Islands,' as the ICIJ puts it.

In December 2011, the London *Financial Times* reported that Lazare Kaplan, the diamond-dealing giant, was "suing two Belgian banks for allegedly stealing $135m in diamond sales by funnelling the proceeds through numerous shell companies across Europe, the Middle East and Asia." The complaint, a civil one made in a US court which Offshore Red has seen, implicates Daleyot and asks for a jury trial to be convened, although it does not name him as a defendant. Lazare seeks redress under the *Racketeer Influenced and Corrupt Organizations Act (RICO)* for catastrophic damages to its business that were caused by a racketeering, fraud and money-laundering scheme conducted by banks KBC and ADB, in concert with a complex web of individuals and entities controlled by or associated with Daleyot, who was their customer. The two banks and Daleyot's entities allegedly stole and diverted in excess of $135 millions' worth of diamonds that Lazare and its affiliates had bought or financed.

"Leaked files show that HSBC overlooked Arcadi Gaydamak and 'Jacob the Jeweller'"

This is nothing new, but the leaked files also show that HSBC overlooked plenty of Daleyot's unsavoury associates, especially Arcadi Gaydamak, a Russian-born Israeli business magnate convicted in absentia in France of organising arms trafficking in Angola during the civil war in 1993-1998 in the amount of $790 million in contravention of international law. Daleyot also funded his friend, Jacob 'the jeweller' Arabo, who later admitted to submitting a false document to the federal authorities attesting that pieces of jewellery had simply been lent for a video shoot when in fact they had been sold. At one time, the records show, HSBC held accounts for 2,000 people in the diamond trade, many of them with murky associations and/or subject to police investigations, according to the ICIJ; the bank ceased to have customers from this sector in 2013. A Belgian prosecutor charged HSBC's Swiss unit in November with fraud, money laundering, and criminal conspiracy, most of it connected to customers who made their living from the diamond trade.

Conflict diamonds are a factor here. An HSBC diamond-dealing customer named Emmanuel Shallop was mentioned in a 2001 United Nations report for doing business with the rebels in Sierra Leone's civil war, but this did not stop the bank acting for him. In 2010 he was convicted in Belgium for facilitating 'blood diamond' trades involving dozens of millions of dollars.

HALLIBURTON'S AFTERMATH

Then there are fresh revelations about the old story of the British tax lawyer who used HSBC accounts in his name and those of members of his family to facilitate a $182-Million Halliburton bribery scandal in Nigeria. Jeffrey Tesler pled guilty to US bribery charges in 2012 saying, much as HSBC is saying about all the recent leaks, that he 'made mistakes' and 'didn't look'. He used bank accounts in offshore tax havens to funnel bribe money to Nigerian officials who then authorised $6 billion worth of construction and other contracts. The newly publicised files show links between Tesler and other Nigerian officials whom he did not name while negotiating with the Americans. These were Major General Chris Garuba (chief of staff to the president and a former governor of Northeastern Bauchi state) and Andrew Agom, a board member of the ruling party, the latter now deceased. The major-general at least was a classic 'politically exposed person' whose involvement should have attracted 'extra due diligence' at all banks that encountered him or his 'close associates'.

Unfortunately, Nigeria's government has not taken action against the officials at the receiving end. Also of note is the fact that in 2010 Nigeria indicted former US Vice President Dick Cheney, who was the CEO of Halliburton before 2000, over the affair but absolved him later when Halliburton worked out a $35 million settlement. Cheney is the only sitting 'veep' to shoot someone since Aaron Burr killed Alexander Hamilton in a duel in 1804.

Another name that keeps popping up in the HSBC files on Nigeria with astounding regularity is that of Abu Shuaibu. Nobody seems to know who he is, but the files say that he was the beneficial owner of an account named Bridlington Enterprises Ltd, a Gibraltar-based shell company for which Tesler acted as a lawyer. Bank records show him as a real estate dealer whose address is PO Box 53322, Ikoyi WANLagos. Shuaibu and Tesler seem to have been linked to each other very strongly and may have worked together.

The fact - exposed in *Le Figaro* in December 2003 - that Tesler was under investigation did not stop HSBC from advising him. The bank must have known he was a mere lawyer, yet he and his family had tens of millions in their accounts in 2006-7. Neither his wife Judy nor his daughters have been prosecuted. Judy at one point 'owned' $35 million. The leaks say that one daughter, Laura, was a student at the time with no visible means of support and became a millionairess overnight. She was the beneficial owner of an account in the name of a Panamanian company that held almost $4 million. In 2005 Judy Tesler ordered some buying and selling activity on an account to the value of $380,000. HSBC should not have done her bidding as the account was frozen under a court order that stemmed from the publicly known investigation, but it allowed the sale of the investments anyway. Far from reporting a crime, as was its legal duty, the bank seems to have performed one.

CAUGHT OUT

One small revelation concerns a British HNW client called Keith Humphreys, who was a director of Stoke City FC. Notes in one file refer to him telling his HSBC RM that one of his family's Swiss accounts was 'not declared' to the Inland Revenue. According to the file, it held $450,000. Recently Humphreys told the Guardian that the account was in the name of his father and that it was "disclosed to British tax authorities in 2011, with a settlement of £147,165," suggesting that the British tax authorities knew that something was up.

PULLING AMERICA'S GOLDEN CHAIN

The 'Golden Chain' was a list of purported sponsors of Al Qaeda that Bosnian police seized in March 2002 in a raid of the premises of the Benevolence International Foundation in Sarajevo. Osama bin Laden had been known to refer to it warmly. The list was of 20 top

Arabian (Saudi and otherwise) financial sponsors of Al Qaeda, including bankers such as Khalid bin Mahfouz, who died in 2009, and businessmen and former ministers. Everybody in the money-laundering world knew of the list by spring 2003 and yet, according to the ICIJ, HSBC was still processing accounts for at least three people on it after 2003. Carl Levin, the chairman of the US senate committee that spearheaded the $1.9 billion fine of December 2012, stated the US law most clearly: whenever HSBC or any bank encountered anyone on that list, they should have 'taken notice', classified them as highly risky clients, and trimmed their relationships accordingly. This they do not seem to have done.

PROSECUTIONS PENDING?

HSBC is looking more and more like an international crime syndicate. Criminal prosecutors in Belgium, France and Argentina are now investigating the Swiss unit of London-based HSBC and some of its customers. A former HSBC employee called Hervé Falciani seems to have 'blown the whistle' in the Belgian case, in which HSBC stands accused of no less than outright money-laundering in its efforts to help 1,000 Belgian HNWIs commit tax evasion. At the same time, the Australian Taxation Office says that it is investigating 'discrepancies' in accounts that HSBC held for Australians in those far-off days. Civil cases also allege its involvement in the rigging of gold and silver prices.

"The SEC has recently fined HSBC's Swiss arm for doing unregulated business in the US"

Regulators, too, have been giving HSBC a hard time ever since the mega-fine of $1.9 billion - almost five weeks' revenue - that it had to pay in 2012 for ten years of money-laundering. It has had to pay £618 million to British and American regulators for illegally fixing rates and is being pursued by the US Federal Depositary Insurance Company for more, and the US Securities and Exchange Commission has recently fined its Swiss arm for doing unregulated business in the US.

HERE AND THERE

Another interesting revelation concerns the self-classification of wealthy customers at HSBC's private bank. An amazing number - more than 7,300 - described themselves in the files as 'housewives.' (Less than 4,000, by contrast, were classified as 'without profession' or 'student', which were other favourites.) Mary Wells Lawrence, an advertising guru and the first woman to be in charge of a corporation listed on the New York Stock Exchange, so described herself. She lived in a mansion in Mustique and held two accounts at HSBC, one in the name of a Bahamas offshore company called Five Angels Investment, and another called Scandia Corporation. About $140 million resided within. Other atypical 'housewives' included Saudi Princess Lolowah, a now-deceased Thai-businesswoman-turned-fugitive called Khunying Patcharee Wongpaitoon, and septuagentarian fashion heiress Arlette Ricci, who was actually a theatre director, with more than $20 million in the account of a company registered in Panama. This last lady was reportedly charged with tax fraud in France because of undeclared Swiss accounts. The word 'housewife' might be viewed as more of a 'red flag' than as a badge of domestic simplicity if these files are anything to go by.

The ICIJ has also published verbatim accounts of HSBC staff, usually relationship managers it appears, writing about their clients. They touch on a need for discretion that regulators sometimes neglect, i.e. security worries that high-net-worth individuals have, as evidenced in these quotations:

- "We are prohibited from calling the client in Belgium. It's always him who calls us. He telephoned today. He introduces himself under the name of a footballer (Johann Cruyff); wants to know the "price of caviar," which means the total value of his assets."
- "Mentioned they are very concerned with confidentiality and security, his wife has already been kidnapped right after their marriage and was found by the police…brother has also been kidnapped."
- Another quotation typified many, this time on a darker theme: "I again indicated that we were not tax inspectors."

All human life is here. The ICIJ is not providing a link for a full downloading of the files. This may be because it wants to gain some sort of commercial advantage. The public may have to wait for more selective leaks through newspapers such as Le Monde and the Guardian.

LABOURING A POINT

Ed Miliband, the leader of HM Government's Labour opposition in the UK, has promised a raft of tough taxes against offshore centres and a crackdown on tax loopholes for the wealthy and big businesses, but this is because an election is approaching. The details of his promises are hardly worth a mention. We have been here before, with Labour's Gordon Brown promising in opposition to end the 'non-dom' rule in the 1990s. In 2008, after Brown had been chancellor for a decade and then moved on to become prime minister, Alistair Darling, his successor, imposed a mere £30,000 annual charge on all non-doms, which was subsequently bumped up to £50,000 – the kind of money that the average ultra-high-net-worth individual spends on a party for one of his children.

Labour's anti-tax-abuse record is hardly spotless in any case. It received £386,000 in donations from PricewaterhouseCoopers – one of the foremost firms accused of facilitating 'aggressive tax planning' and Labour's biggest donor outside the trade unions. PwC has also donated generously to the Conservative Party, according to the Electoral Commission.

Another recent revelation is that Michael Bloomberg has given more than £500,000 to the UK's three main political parties through one of his companies, which either suggests that he cannot make his mind up about politics or that there is little to choose between them by way of policy.

Anthony Travers, the chairman of the Cayman Islands stock exchange, had this to say to *Compliance Matters*: "OECD Secretary General Mr Angel Gurria has stated that companies cannot be blamed for taking advantage of lawful tax avoidance and indeed it is to domestic tax legislation on transfer pricing (ironically based on the OECD model) that Mr Miliband should look if he wishes to capture the 'billions' to which he refers.

"An informed politician, genuinely concerned about tax evasion and tax avoidance, as opposed to making populist sound bites, should be lauding the standards of transparency set by the UK's overseas territories as the example to which other jurisdictions, notably the wholly opaque US corporate centres of Delaware, Wyoming and Nevada, should now be held. He should also be making more detailed enquiries about the double-tax treaty abuses that are a matter of routine in the European centres." ■

THE DANGERS OF BITCOIN: SOME MYTHS DISPELLED

Bitcoin, as readers will know, has often been touted as a radical new alternative to today's failing fiat currencies. In the last year we have seen virtual currency exchanges flee the stifling regulatory environment of New York for the 'light touch' regulation-to-be of the Isle of Man, the announcement of Singapore that it wants to regulate, and much more besides. Is virtual currency as criminogenic as its critics claim? Siân Jones, the regulation and compliance specialist at the virtual currency consultancy of COINsult, debunks some of the myths that surround virtual currency in general and Bitcoin in particular.

People say - and this is a cliché of the first order - that Bitcoin is an anonymous virtual currency. This is simply not true; instead, it is a pseudonymous network. Everything is very transparent in the blockchain. Everything is recorded widely and is there in full public view. The realworld identity behind a Bitcoin address is not on public display (and when I say 'Bitcoin' in this article, I am usually talking about all virtual currencies, of which Bitcoin is the first and perhaps might turn out to be the best) but a competent investigator can follow the life of a Bitcoin more accurately than he can follow the life of a banknote. In the United States, every bank is required to 'capture' (i.e. log) the serial number of every $100 bill that goes through its doors. That means that $100 bills are not traceable between people, but they are (if the banks do their job) traceable through every bank they have been through. The way Bitcoin works allows for even better surveillance than this.

"Using correlation, an AML investigator can pinpoint a real-world identity"

A Bitcoin wallet contains one or many Bitcoin addresses. On the face of it, one cannot necessarily know to whom a Bitcoin belongs. We live in a world where states believe that money-laundering is bad and should be suppressed and those states usually impose constraints on market participants in their quest to clamp down on it. Typically, banks dominate the world's payment systems and do jobs on behalf of the states under whose licences they operate. There are 'choke-points' that allow them to collect data, such as the physical arrival of a $100 bill at a bank, and it is the same in the Bitcoin world.

VIRTUAL CHOKE-POINTS

Virtual currency exchanges provide a good example. A natural 'choke-point' occurs whenever one of these organisations swaps digital currency for fiat currency and vice versa, or when it swaps one crypto-currency for another ('cryptoto-crypto'). There are other obvious examples. Some businesses act as online wallet providers, relieving the user of the necessity of keeping a wallet on his own computer of mobile device that he might lose (although there are ways in which he can mitigate the risk of this). Such guardians or 'monitors' keep Bitcoins in a way that is analogous to gold deposits in a medieval smithy, with the slight difference that the smiths issued promissory notes to repay the gold out to the public, but did so in multiples.

The transparency of the public ledger, i.e. the blockchain, prevents the 'walleteers' from playing the same game. Then there are businesses that put virtual currencies offline into 'cold storage', operating something that resembles a deep gold vault that cannot be hacked and that often operates in an insured environment. In the forefront of this activity is a British company called Eliptic.

You could decide how far and wide to extend that. You could include real-estate agents or high-value goods dealers. You would have a threshold, as with real money. Again, such a course is not without its problems. You cannot know if the holder who is sending you your Bitcoin to store or exchange is using clean money in the first place, but then you cannot know that with cash either. The way to get around this problem, as all know-your-customer regimes do today, is by asking questions about his motives.

"Perfect anonymity may be impossible; forensic tracing software already exists"

You can launder Bitcoins by mixing them with others and spilling them out in different directions. Although so-called 'mixing services' do exist which combine Bitcoins belonging to the user with those belonging to others and which therefore obscure the flow of funds, it can be a very complicated job to cloak one's operations in reasonable anonymity. Perfect anonymity, indeed, may be impossible. Forensic tracing software already exists and more sophisticated tools are on the way.

THE DECLINING PROBLEM OF TRACEABILITY

On 25th November Alex Biryukov of the University of Luxembourg published a paper on the de-anonymisation of clients. In it, he demonstrated that shared funds that had been laundered were still traceable. According to another study, it is easy to link up IP addresses to each Bitcoin address. On the money-laundering front, things are already looking better for Bitcoin than they are for cash.

Using correlation, an AML investigator can pinpoint a real-world identity. He can find some point of contact with a real organisation like Waterstones that will, in the face of a warrant, be obliged to reveal the identity of the individual to him. Unless the investigator is following marked banknotes, he cannot do that with cash. Bitcoin is therefore considered easier to trace than paper money. There is no Bitcoin equivalent of the notorious €500 note which, when first issued more than a decade ago, became an untraceable boon for money-launderers, especially on the Costa del Sol.

TRACEABILITY TOOLS - COMING TO MARKET IN 18 MONTHS

There probably are one or two firms that offer forensic tools that allow investigators to trace Bitcoins in this way, but there are as yet no 'common or garden' products on the market. Most of the tools that can do this have been created at research level. One company - Matrix Vision (under Marco Crispini) - is working on something that will interrogate the blockchain that can almost be described as a monitoring tool to trace flows of funds across the blockchain. Matrix already makes tools for KYC and digital currency. It also

makes a 'customer relationship management' system that is tailored to the consumer's needs and links up with KYC tools. At the moment, however, the lack of regulation ensures that few people are motivated to produce such tools for the market. This situation, however, is liable to change in the next year to 18 months.

TOPPLING EXCHANGES - THE WAY OF THE PAST?

Another problem with Bitcoin's image is that it is thought to be 'hackable.' Critics of cryptocurrencies make great play of the demise of Mt Gox in February 2014 and the recent Bitstamp hack, in which a British exchange suffered a distributed denial-of-service last month. Bitstamp is the largest Bitcoin exchange in Europe and one of the longest-established. Someone hacked its wallet, which was a 'cold wallet', i.e. keeping Bitcoins in 'cold storage' and not online. The hackers robbed the wallet of less than 19,000 Bitcoins or $5 million, which is fairly small beer. This operation is hardly an indictment of Bitcoins and their exchanges any more than a straightforward bank robbery is an indictment of money and banks. To continue the analogy of a bank robbery, the intruders managed to plunder one of the tills but not the safe. Indeed, the exchange managed the whole affair very well, preventing all its 'hot wallets' from being raided. The raid happened over several hours and was noticed reasonably quickly.

"The failure of Mt Gox happened through sheer incompetence"

On the same day something much more serious happened - the online greeting card service Moonpig had to suspend its mobile apps because someone discovered a security flaw that endangered 3 million customers' account details. In fact, a developer called Paul Price told Moonpig about its gaping security problem 17 months earlier and only now went public, frustrated by the company's refusal to respond. This, unlike the Bitstamp hack, is the profile of a real security problem.

The failure of Mt Gox, by contrast, was a catastrophe that happened through sheer incompetence on the part of its management. It is possible, although nobody has proved it, that the theft of 850,000 Bitcoins belonging to customers (valued at more than $450 million at the time) could have been an 'inside job'.

THE DARK SIDE OF THE WEB

What of Silk Road, the online black market, best remembered as a platform for selling the kind of illegal drugs that the US Government only wants the Central Intelligence Agency to sell? It is certainly true that anybody who does not like the idea of private individuals outside the CIA selling these drugs to the public will probably be hostile to, and perhaps even disturbed by, the existence of such an exchange. It is a fact, however, that in spite of the paranoia about anonymous Bitcoin-based websites frustrating investigators, the Federal Bureau of Investigation was able to conduct a good investigation that led to copious seizures and the apprehension of Ross William Ulbricht, the website's founder. Silk Road is not a dire warning about the dangers of Bitcoin; it is the story of a triumphant investigation.

THE REALLY INTRACTABLE PROBLEMS

Bitcoin does have some problems. At the moment, for a number of reasons, the number of people who provide the network capability for Bitcoin is growing smaller and smaller. This is one reason why Bitcoin might not be the virtual currency that dominates the scene in the end.

"Silk Road is not a dire warning about Bitcoin; it is the story of a triumphant investigation"

The question of whether Bitcoin's encryption is safe is a simple one, but the answer to it is complex. Bitcoin is an 'open source' project - this is one of its greatest features. It relies on published code. This means that anybody can attack it. A very large number of people are out there proving and testing it, making it stronger.

This, however, is not an advantage that banks have. For 3 years, the subsidiaries of Royal Bank of Scotland, Natwest and Ulsterbank suffered a failure that made their systems inoperable. This, in turn, caused a great deal of damage to people's lives because payments stopped being made. RBS was fined. Two years ago, it was the Bitcoin network's turn to suffer a fault. Within half an hour, people were working all over the world to fix it. Core developers and some of the larger players such as Mt Gox got together from around the globe and fixed the problem because it was open-source. A change in the code was effected very quickly, so the whole episode ended up as a minor hiccup rather than a major 'outage'. In other words, the solution had the consensus of enough people to work and that is how the Bitcoin universe prospers.

I do not think that the banks of today believe that Bitcoin will prove to be a money-laundering currency. It is not going to take over from the real-world currencies, so it will not be important enough to justify many of the fears that surround it now. Instead, it promises to be a boon to the 'unbanked' of the Third World and will solve many of today's offshore payment problems. ■

** Siân Jones can be reached at sian@coinsult.eu or on +44 115 824 0019*

NEW RULES FOR A NEW FINANCIAL CENTRE

The Abu Dhabi Global Market is moving into offshore financial services this year. The jurisdiction at present focuses on oil and gas but it hopes to remedy this with the ADGM, its free-trade zone which, according to reports was 'created' in 2013 but has not yet been 'launched'. Cabinet Resolution No 4 of 2013 called for the setting-up of the financial free zone on Al Maryah Island and Law No 4 of 2013 established the ADGM and its board of directors as its authority. The big news is that the ADGM is eschewing the Code Napoleon for English common law as its legal base. Abu Dhabi and the United Arab Emirates civil and commercial law will not apply in ADGM, but the federal criminal law of the UAE will. British, Caribbean, Australian and New Zealand law firms, ex-regulators and compliance consultants are reportedly rubbing their hands in anticipation.

Sir Hector Sants, one British former regulator who has seen better days, has been appointed the chief advisor to the chairman, Ahmed Al Sayegh. The ADGM board seems to have fought shy of giving Sants any executive responsibility after his stressful breakdown at Barclays.

Canada

PAYMENT FOR INFORMANTS COMING TO CANADA

For the first time in Canada's financial services industry, there is to be a regulatory policy for informants to rival that of the United States, although even the American 'whistleblowing' regime is in its infancy. The Ontario Securities Commission (OSC) has released Staff Consultation Paper 15-401, which proposes a new initiative to encourage the reporting of serious misconduct in violation of Ontario's securities law to the regulator. Incentives could range up to C$1.5 million upon the final resolution of an administrative enforcement matter. ■

Singapore

COMPLIANCE JOBS AND SALARIES SURGE IN LION CITY

Job advertising volumes for Singapore-based compliance and legal jobs skyrocketed by 64% in the final three months of 2014 from a year earlier, as regulatory pressures mounted on sectors such as wealth management, new figures show.

The Lion City was confronted with an 'acute talent crunch', resulting in a flurry of advertisements for human resources professionals, with ad volumes surging by 48% year-on-year, according to Robert Walters, the international recruitment firm, in one of its regular overviews of the Asian employment market.

The data would seem to confirm anecdotal evidence about a boom in compliance-related jobs and the salaries of such positions. As financial markets have been affected by a wave of regulatory action and scandals such as benchmark-rigging and money laundering, so demand for such positions has also surged.

Singapore is far ahead of the rest of Asia for such compliance and legal ad volume growth. Throughout the whole of Asia, the report said, advertising volume for jobs in legal and compliance functions rose by 10% in the final three months of 2014 from the same period a year before. Accounting and finance job ad volumes rose 27% in Asia, the firm said. The Robert Walters Asia Job Index tracks job advertising volumes for professional positions across the leading job boards and national newspapers in China, Hong Kong, Japan, Malaysia and Singapore.

In China, accounting and finance job ad volumes rose 26% year-on-year. In Hong Kong, a rival wealth management hub to Singapore, such ads rose by a robust 43%, the report added. ■

United Kingdom

COUNCIL CONSULTS BANKS ABOUT EXCHANGE OF TAX INFORMATION

The Swiss Federal Council has begun consulting interested parties about the international exchange of tax-related information with the publication of two documents.

Two bills are involved. One concerns the Organisation for Economic Co-operation and Development/Council of Europe administrative assistance convention signed by Switzerland in October 2013. The other bill concerns Switzerland's participation in the Multilateral Competent Authority Agreement and the *Automatic Exchange of Information [AEOI] Implementing Act*. Parliament will be asked to pick out the countries with which Switzerland should exchange information automatically at a later, separate stage.

The 'administrative assistance' convention makes provision for the three forms of information exchange: upon request, spontaneous and automatic. The Federal Council says that it wants to 'exclude' assistance in enforcement and administrative assistance for the service of documents. It is also proposing to make two declarations: firstly, that Switzerland will generally inform affected persons about the forthcoming exchange of information; and secondly, that Switzerland will not allow foreign authorities' requests to conduct tax audits in Switzerland. ■

Denmark

RATE-SETTERS RECEIVE CLEAN BILL OF HEALTH

The Danish Financial Supervisory Authority reported recently that it had carried out an investigation of Copenhagen Interbank Offered Rates in the period from 2009 to 2012. The investigation was based on internal documents provided by Danish Cibor-quoting institutions.

The regulator looked at the following:

- Documents concerning the governance structure of the institutions in relation to the Cibor rate, including procedures, internal controls and incentive earnings.
- Data and sensitivity calculations of the exposure of the institutions to Cibor-related products.
- Internal and external correspondence, including letters, emails, chat messages and recorded telephone conversations regarding Cibor re-ports and quotes.

In its review of the institutions' internal documents regarding Cibor-setting, the Danish FSA found neither documentary evidence of law-breaking nor evidence of 'activities of a manipulative character'. Therefore, as a result of the investigation, the Danish FSA found no reason to tell the Danish Competition and Consumer about offences against the *Competition Act* or to tell the Public Prosecutor for Serious Economic and International Crime about any financial offences.

Some documents indicate that various financial institutions were aware that they had an interest in common with others in keeping the interest rates high, but the gains to be made were still trifling. ■

Cayman Islands

LIQUIDATION FOLLOWS SEC SUIT AGAINST CAYMAN 'PUMP AND DUMP' BANK

Cayman's Caledonian Bank's shareholders have called in the receivers as a result of the US Securities and Exchange Commission charging it and four other offshore entities with offering and selling unregistered penny stocks into the public markets.

In a writ issued in the Southern District of New York, the regulator is seeking 'disgorgement' of ill-gotten gains, plus civil penalties. The five defendant entities are Cayman Islands-based Caledonian Bank Ltd and Caledonian Securities Ltd, i.e. the bank's brokerage, Belize-based Clear Water Securities Inc and Legacy Global Markets SA, and Panama-based Verdmont Capital SA. The SEC believes that they reaped more than $75 million in illegal sales perpetrated against American investors. The SEC has also obtained an emergency court order freezing whatever assets of these entities are located in the United States.

The SEC alleges that the defendants sold

penny stocks in unregistered distributions from their US brokerage accounts of four shell company issuers, namely Swingplane Ventures Inc, Goff Corp, Norstra Energy Inc and Xumanii Inc. Each of the unregistered distributions took place through virtually the same scheme. The issuers first sent the SEC bogus 'S-1' forms that purported to register sales of securities to public investors when, in fact, no bona fide sales occurred because the securities purportedly sold remained in the control of the issuers and their affiliates. In the sham offerings, the issuers pretended to sell securities to investors residing in such places as Serbia, Mexico, Ireland, Norway, Panama and Jamaica, while the issuers or their affiliates maintained control and possession of the stock certificates in a scheme where:

- restricted stock was passed off as "free trading" unrestricted stock;
- the share certificates issued were subsequently transferred, without restrictive legends, to the defendants; and
- the defendants deposited the shares into their US brokerage accounts and sold them on to the public.

The complaint further alleges that the issuers or their affiliates directed the transfers of restricted securities to the defendants, often through various offshore nominee entities intended to conceal the securities' beneficial ownership. Once the shares, which were controlled throughout by the issuers or its affiliates, were held in names of the defendants, the shell company issuers announced a reverse-merger or business combination with a purportedly operating enterprise. The defendants then offered and sold into the public markets hundreds of millions of shares of the four issuers in unregistered distributions all at once and to the sound of trumpets. Each of the four stocks lost virtually all of their market value within months. ■

Germany

A NEW HEAD FOR THE BAFIN

Felix Hufeld, currently Chief Executive Director of insurance supervision, is to become the new president of the BaFin. He will take over from Dr Elke König at the beginning of March. Dr König will be moving to Brussels to help set up and head the EU's so-called Single Resolution Board.

Since the 1930s, 'resolution' has been the word that describes what the US Federal Deposit Insurance Corporation does when a bank it has insured fails. FDIC bank supervisors determine that the bank's assets are worth less than its liabilities, then the bank itself is shut down and its assets are transferred to a new entity controlled by the FDIC. The word 'resolution' seems to have the same meaning in the jargon of the European Union, i.e the winding-up of institutions.

Hufeld has been the head of insurance supervision at BaFin since January 2013. He is also chairman of the Executive Committee of the International Association of Insurance Supervisors (IAIS) and a member of the management board and the board of supervisors of the European Insurance and Occupational Pensions Authority (EIOPA). No stauncher supporter of the European Union could be found.

His female predecessor, Dr Elke König, recently said that the European Union's Single Supervisory Mechanism's standards of supervision made sense, but added that the standardisation of regulation and supervision must not degenerate into a 'levelling down' process - in other words, rigorous German practices must prevail over sloppy east and south European ones. The European Central Bank is leading this centralising initiative and the idea is to give the ECB specific supervisory and rule-making powers over credit institutions in Euroland. The SSM is open to the participation of other EU countries that wish to join, but none does.

National regulators are to retain some functions under the new regime, but the ECB will directly supervise banks with assets of more than €30 billion, banks that earn at least 20% of their home country's GDP or banks that have asked for or received direct public financial assistance from the EU.

Once the SSM is up and running, the ECB will be responsible for the supervision of all 6,000 banks of the euro area. The decline in the number of banks in the EU has been noticeable in recent years - in 2013 the figure was 152 banks and other lenders, according to the ECB.

König, and presumably Hufeld as well, believe that the EU's Single Resolution Mechanism (SRM) will make EU-wide 'banking union' complete and make the winding-up of systemically important banks more orderly as well. König likes the idea of Euroland having a highly centralised 'resolution' regime but she has also called for a global one. The idea of British taxpayers stumping up for failures at Brazilian banks might strike some as a trifle odd; Hufeld's opinion on the matter is not known. ■

Jersey

FATCA NOW 'LIVE' IN JERSEY

Jersey's 'foreign financial institution' reporting system is now up and running. The bailiwick's financial institutions are now able to register there in preparation for the US *Foreign Accounts Tax Compliance Act*, which comes into force this year. *FATCA* requires financial institutions outside the USA to report information on financial accounts held by their US customers to the Internal Revenue Service (IRS) or, in the case of Jersey, to the Comptroller of Taxes who will pass it on to the Americans.

A test platform has been available to local financial institutions since last month to test their file formats and help them familiarise themselves with the *FATCA* return process. Now financial institutions can register on the live system and submit information required under the *FATCA* rules. The Comptroller of Taxes, acting as Jersey's 'competent authority' under the intergovernmental agreement it signed on 13 December 2013, requires the information to be submitted by 30 June each year.

Financial institutions in Jersey should have already registered with the IRS in order to obtain a Global Intermediary Identification Number (GIIN). When registering in Jersey they must enter the GIIN and other information, including a designated point of contact. Someone in the Jersey Government - the Government's website does not say who - is writing up two sets of guidelines. The first are general and are to be the same as those from Guernsey and the Isle of Man.

More than 100 IGAs now exist between the US and other governments. This has not, however, stopped the IRS from relaxing various parts of its ultimata further. It now means to treat various countries as though they have IGAs in force even if they have not. In a circular issued in November, it said: "This announcement addresses these concerns by providing that a jurisdiction that is treated as if it had an IGA in effect, but that has not yet signed an IGA, retains such status beyond December 31, 2014, provided that the jurisdiction continues to demonstrate firm resolve to sign the IGA that was agreed in substance on or before June 30, 2014, as soon as possible. After December 31, 2014, Treasury [Americans never call it 'the Treasury'] will review the list of jurisdictions." ■

smartKYC

The smartest way to know your customer

A semantic engine for KYC and AML due diligence

Getting a full picture of potential clients - both individuals and business entities - is becoming increasingly hard for the private client world.

But now a solution is at hand. smartKYC has applied innovative design and technology to redefine KYC searches and identification of AML red flags.

Applying semantic technology, federated searches and intelligent techniques to detect false positives, the smartKYC AML suite increases the precision, efficiency and auditability of your KYC and AML efforts.

CYBER-CRIME: EXPECTED TRENDS FOR 2015

The Internet is a very dirty place, and about to get dirtier. What should private banks, trustees and fund firms do to protect their operations and data?

Paul Stokes, the chief operating officer of Wynyard Group, along with Andy France, the group's chief intelligence advisor, spoke to *Compliance Matters* about the cyber-security threats that many compliance departments are having to deal with. This article is the result of that interview. Financial firms would do well to heed their predictions for the year ahead.

* More and more firms will realise that no company is immune to cyber-attacks and that so-called perimeter security is no longer enough.

Today, organisations operate in a perimeter-less cyber-world and the idea that an organisation can throw a fence up at its edge to protect its inner parts is fiction. Many organisations continue to use security software (we cannot say whose for legal reasons) from the 1990s, which is useless. Sophisticated cyber-criminals have rendered traditional 'perimeter defences' such as proxies, firewalls, virtual private networks, and antivirus and malware tools ineffective.

A few years ago, a traditional company would have an IT department and all the software would be on its own machines. Then came the Internet, to which everybody wanted to be connected. This widened the threat horizon to take in all people who could be connected to each other by 'phone. People overseas were now connected to it in large numbers. The traditional company could keep locks on its old system but this did not make sense in a world where everybody was connected to everyone else.

Think of cyber-security as though you are planning to fortify your house. You can put locks on the windows and doors, perhaps also buying a burglar alarm and joining the Neighbourhoood Watch. If you do all that but leave your back door open as well, you only have yourself to blame. Cyber-security always was like that, but now people are digging through the wall! People are dismantling the roof! A wall, or a moat, does not work any more. Companies now need to detect threats inside the firewall and as they develop.

In today's threat landscape, organisations face extremely sophisticated intruders who continually upgrade their skills. The means by which they can penetrate networks, and conceal their presence within those networks, are legion. When a criminal steals a manager's credentials, he looks like the manager – he is, after all, logged in as him. In cyber-crime, it is a good idea to steal identities. One of the hardest things to find in cyber-security is someone using someone else's password and appearing as them. 80% of all personal identification number (PIN) words are used by people for everything, that is to say that the typical person uses the same PIN for his phone, his cash card and everything else. The capabilities of insiders who abuse their access rights to manipulate and steal data should not be forgotten either.

Is cyber-security better in the securities and banking world than in, to take a random example, the insurance and life policy world? One might expect there to be glaring differences between these sectors but in fact there is little difference. No sector of financial services is as advanced as the people who are orchestrating attacks. All one can do is try to build more perimeters, meet the attackers inside the system and have tools to deal with them before they do damage.

Attacks often remain undetected until it is too late. Many uninformed bystanders believe that all cyber-attacks are over in a flash. This is a common misconception. To use a medical analogy, one develops the symptoms of catching a cold before he progresses to full-blown pneumonia. He has time to go to a doctor to ameliorate his condition. The process of lifting data out of someone else's system also takes time. The IT manager can spot the symptoms before the deed is done. This is a new way of thinking. It uses new technology and that technology is used for diagnoses as well as cures – it is impossible for a human to keep up now.

* Firms will have to invest more heavily than ever before in cyber-intelligence software that allows them to detect threats and respond to them rapidly.

According to Gartner, by 2020, 60% of enterprises' information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2012. Some governments are no longer relying on the implementation of information security policies or traditional perimeter cyber-security tools. They are now actively "building cyber-intelligence capability" to reduce the "unknown unknowns" that are likely to affect their operations or economies.

One such government is that of the UK, which has its own cyber-security strategy. Other countries are doing the same. Wynyard deals with governments itself but does not want to identify them or the tasks it performs for them. Things used to be rules-based, but governments are now realising that they have to take a step back and take a risk-based approach, spending money on the more risky areas of cyber-security. Cyber-intelligence capability involves human planning, not leaving it up to a machine.

Technology has gone so far that there is a dearth of talent at large firms, so the limited number of people with the right skills have to work on the most important risks. The most skilful people often come from the government. [Editor's note: they also come from outfits such as CSG Government Solutions, which look after HM Government's systems. The pay at CSG is reputedly less than at some of the bigger consulting firms.] The government also encourages universities to sponsor cyber-security degrees – another source of skilled workers.

* The rôle of the Chief Information Security Officer (CISO) will become more important.

CISOs at financial firms are being "invited to the top table" more often as time goes on. This is an admission that in many cases a business's survival relies on the security of its technology. Organizations are now tending to elevate their CISOs to a par with their chief information officers or CIOs. This gives these cyber-security experts an equal voice in the formulation of resource-related priorities and decisions about various risks.

Is this a conscious policy, born out of careful research and consequent board decisions to take cyber-security more seriously? To some degree the answer is no; it is happening automatically. One

tends to find that when security has been breached and things have gone spectacularly wrong, it is because a junior person has been given responsibility for cyber-security. During the times when the company ought to be preparing for attack, in the lulls between emergencies, top directors tend to ask their IT people leading questions about whether security is good enough at the moment, while also putting pressure on those same people to say 'yes, of course.' This is a recipe for disaster rather than good and timely problem-solving. Indeed, this is one of the most pernicious problems of cyber-security. The only remedy is to have someone senior in charge of security who can argue with/contradict his peers on the board from a position of equal status.

Another misconception that our corporate public has is the assumption that when cyber-attacks happen to them, their companies were targeted. Actually the process is fairly random – criminal software spends its time looking opportunistically for any weakness at any address.

* There is – and will continue to be – a massive shortage of people with the right 'cyber security' skills.

After a year in which many high-profile companies were hacked, financial firms are spending more on cyber-security and increasing the size of their cyber teams. There is no known research on which sectors are spending more than others as a percentage of turnover, or whether large firms are spending a smaller proportion of their turnover on it in the same way that they do with compliance. Having said this, it seems likely that economies of scale apply.

People who have direct, first-hand experience in identifying 'cyber risks' and improving organisations' defences against them are in high demand but the supply of these people is low and this will get worse as security teams increase in size.

* Governments and private enterprises will collaborate more to tackle cyber-threats.

The cyber threat landscape is changing rapidly. Governments are taking such steps as the Australian cyber security review to improve the defence of our businesses and crucial national infrastructure. We shall see this trend gather pace, with governments increasingly acknowledging their need to work with the private sector in the face of this growing problem.

The biggest change for many financial firms in recent years lies in the fact that the greatest asset they own is now intellectual property that resides in the data about customers that they store. This data is so valuable that it is no exaggeration to say that our financial business has moved from physical wealth to digital wealth. Criminals who attack this are increasingly sophisticated – they take a 'supply chain' approach.

For example, there is a huge black market on the Dark Web, formerly known as the Invisible Web. Our research suggests that it costs $103 to buy a credit card number and code that will allow the purchaser to siphon money out of a bank account. There is a large market for other data such as commercial secrets. Some companies, it is true, will reject any offers from criminals to sell them their competitors' plans or customer databases, but many will not. The manufacturing market is full of exact replicas of inventions to which copyright applies. This happened happened to Lockheed Martin, the aircraft company. It also probably happened to a species of Landrover, as a Chinese manufacturer has mysteriously begun building models that are very similar. In last year's Bitcoin Silk Road scam, someone bypassed the site's escrow service and dealt directly with one seller named "Tony76". This shortcut led to the disappearance of 20,000 Bitcoins in less than two weeks.

As we have said, the official Australian cyber-crime review is good, as is the UK's co-ordinated cyber-security strategy. The fight against cyber-crime is not just an Anglo-Saxon initiative, however – Europol, located at the Hague in Holland, has taken down some criminal websites, with police from Romania and Slovakia helping. [Editor's note: On the subject of private-public partnerships, Europol's European Cybercrime Centre has just signed a memorandum of understanding with AnubisNetworks, a cybersecurity and threat intelligence IT company, with the aim of fighting cybercrime. The MoU will facilitate the exchange of expertise, statistics and other strategic information.]

* Cyber risk management will become a priority for the boards of financial firms, if it is not one already.

One thing to note here is that some boards at financial firms – we cannot say which – are thinking of moving responsibility for network security from audit committees to risk committees. These days, cyber-security is coming to be viewed as a business risk rather than a compliance issue.

As we have said, people on the boards of firms have to shoulder responsibility for security policy. Organisations have to understand what their risks are and only senior people can be confident of a fair hearing. Board directors have to ask what attacks their companies have been experiencing over time rather than merely looking at trade press articles. This, too, represents a change – each firm must review everything that has happened to its own systems; there is no other good way to guard against attacks.

* The average firm will spend more time scrutinising other firms that supply it with crucial ancillary services or hold sensitive information on its behalf.

Many organizations do not assess the security practices of supply chains and so-called 'third-party partners' adequately. At the moment, most organisations do not include security provisions in contract negotiations with external vendors and suppliers but they should – we cannot, however, give any examples of firms that do this. Suffice to say that it is imperative for organizations to hold 'third-party partners' to the same cyber-security standards that they set for themselves, if not higher standards.

* Companies will react to 'cyber-events' in a more mature manner as those threats become more commonplace. Companies will also come to believe that security and privacy is everyone's problem.

Companies are increasingly admitting that advanced 'cyber-threats' are an insoluble problem, but they know that the benefits of being connected to the internet outweigh all the risks. Cyber-security is a responsibility shared and managed by all — the public sector, the private sector, and the general public. Some might think that this calls for a revamping of the Internet but, at the moment, nobody owns the Internet and it seems unlikely that people will give up on the present version.

[Editor's note: a Californian company, Javelin Strategy and Research, has looked into the problem of criminal networks harvesting personal data for the purpose of fraud. Their report, published in February 2014, states that "nearly one in three data breach victims in 2013 also became a fraud victim in the same year. This is up from one in four in 2012."] ■

ALGORITHM AND BLUES: A TIGHTENING OF THE AUTOMATED TRADING RULES IS LOOMING

The rules that surround algorithmic trading are increasing compliance activity in the front offices of trading banks and other firms on an unprecedented scale. It remains to be seen whether the current measures will create harmony or discord, writes David Hayes, an associate at CCL, the compliance consultancy.

Not every financial regulatory discussion is given the time allotted to high-frequency trading. The implications of automated trading have been under scrutiny on both sides of the Atlantic for some time, especially since the G20 issued the revolutionary pronouncement that there should be no unregulated financial market and no unregulated financial product.

One of MiFID (Markets in Financial Instruments Directive) II's central aims is to develop stronger rules to govern high-frequency trading. The idea is to oblige high-frequency trading firms to follow a set of 'best practices' and subject then to appropriate controls and oversight. The European Union, from which MiFID comes, also wants to require regulators to license those firms in the same way as brokers.

A SEISMIC SHIFT IN COMPLIANCE

Within Europe, MiFID II (along with the Market Abuse Regulation, or MAR) is expected to create a seismic shift in compliance. Indeed, the compliance function will become a different beast at high-frequency trading firms after 2017. Compliance officers will have to 'sign off' on all algorithms and be responsible for the regulatory requirement for trading surveillance to prevent 'market manipulation behaviours' – and this is irrespective of the size of the firm.

The problem for regulators has always been that regulation should preserve the benefits but mitigate the risks of trading; if they over-regulate, they know that liquidity will disappear.

The American CFTC (Commodity Futures Trading Commission) is also looking closely at high-frequency trading, taking much of its inspiration from MiFID II. Rule 575 issued by the CME Group (an American futures company and one of the largest options and futures exchanges) on the subject of disruptive trading states that traders can only enter orders with the purpose of executing them. Even though this sounds fairly harmless, it becomes extremely potent when we consider that many trading schemes rely on cancelling orders before they are executed.

FROM MAD TO MAR

The aforementioned MAR is replacing the Market Abuse Directive (MAD), which has been in force since October 2004. MAR is meant to lead to a standardisation of rules throughout the EU and, along with the Criminal Sanctions for Market Abuse Directive (CSMAD), will come into effect in July 2016 (although the UK has not yet opted-in to CSMAD). Along with MiFID II there is no transitional period – firms need to comply on Day One.

MAR seems to admit that algorithmic or high-frequency trading strategies can be intrinsically abusive. The market abuse associated with high-frequency trading is typically caught by manipulating transactions or behaviours that relate to 'financial instruments': that is admitted to trading, applied for admission or traded on an in-scope market; or whose price / value depends on, or has an effect on, the price or value of financial instruments.

Examples of manipulating behaviours relates to placing, cancelling, or modifying orders which either disrupt or delay the functioning of the trading system; make it more difficult for others to identify genuine orders; overload or destabilise the system; or are intended to initiate or exacerbate a trend.

INDICATIONS OF MARKET MANIPULATION

MAR Annex I has a list of indications or 'indicators' of market manipulation. They do not constitute market manipulation in themselves, but should be taken into account by market participants and regulators when they are considering transactions or orders to trade. It is on this non-exhaustive list of practices that the European Securities Markets Authority has conducted a consultative exercise (the deadline for replies was 15th October 2014).

Examples include the following practices:

- 'Quote-stuffing' (entering large numbers of orders to trade and/or cancellation and/or updates to orders to trade, creating uncertainty for other participants, slowing down their processes and/or camouflaging one's strategy).
- 'Momentum Ignition' (entering orders to trade, whether or not executed, intended to start or exacerbate a trend and to encourage other participants to accelerate or exacerbate the trend in order to create an opportunity to close out/open a position at a favourable price).
- 'Layering and Spoofing' (submitting many or large orders to trade often slightly away from the market and on one side of the order book in order to execute a trade on the other side, or removing the orders with no intention to execute).

TRUE INTENTIONS

This links directly back to MiFID II and will encourage trading venues to impose fees on firms that have a high rate of cancellations. The ESMA consultative document says: 'Trading venues shall establish economic penalties that are effectively a deterrent and ensure that these penalties are adequately and effectively implemented.'

Obviously, it is always difficult to determine the intentions of traders and work out whether submitted orders were meant to be executed, but new technology makes it easier in some ways to do so. In the old days of 'open outcry' trading floors, the trader carried his strategy in his head and it was not available to scrutiny, but today's trading strategies are well documented in the source code and in the audit trails, explicitly naming all trading signals and the corresponding reactions.

That gives the regulator a much better chance of deciphering a trader's true intentions, even in a complex world like ours. ■

** David Hayes can be reached through the London office of CCL on +44 (0)20 7638 9830.*

THE NEW MAURITIUS INSURANCE STANDARDS: SOME DETAILS

Mauritius' all-in-one financial regulator has published a memo to remind all insurers and insurance brokers of their obligations to uphold its new 'competency standards'. Chris Hamblin of Offshore Red compares it with its British analogue.

When applying for the registration of an insurance salesperson, every insurer must now make a 'statement of declaration' to the Financial Services Commission that attests that he has received 'relevant training'; that he has submitted a 'Certificate of Character'. In the case of an application for a licence by an insurance agent, the insurer must send the FSC the same kind of statement, attesting that relevant training has been provided to the insurance agent or to the designated officer(s) of the insurance agent (i.e. the company); and that a Certificate of Character has been submitted by the insurance agent or the designated officer(s) of the insurance agent.

Insurers must notify the FSC Mauritius, as it likes to be called, of any training they are thinking of providing to insurance salespersons and insurance agents in accordance with Annex 4 of the Competency Standards at least 5 working days prior to the moment the training begins. Insurers have the ultimate responsibility of ensuring that the training satisfies the Competency Standards in every technicality. Insurers must maintain records of any relevant training attended by insurance salespersons and insurance agents, including an attendance sheet of the participants. They must also keep records of the structured CPD (continuous professional development) activity completed by insurance salespersons and insurance agents acting on their behalf. Such CPD records must be made available for inspection by the FSC Mauritius, at any time, upon request.

"Insurers have the ultimate responsibility of ensuring that training satisfies the competency standards"

Insurance brokers and re-insurance brokers licensed before 01 January 2015 have to ask the FSC Mauritius to approve the appointment of at least one designated officer by 1 January 2016.

Upon the appointment of a broking staff, insurance brokers and re-insurance brokers must hand the FSC Mauritius a Statement of Declaration attesting that it is competent and that it has submitted a Certificate of Character.

Insurance brokers and re-insurance brokers must keep records of the structured CPD activity completed by their designated officer(s) and their broking staff. Such CPD records must be made available for inspection by the FSC Mauritius, at any time, upon request.

FITNESS AND PROPRIETY

The Competency Standards are part of the Fair Market Conduct Programme which the FSC Mauritius" or the "Commission") is implementing. In these standards, 'broking staff' has the same meaning as in the Insurance (Insurance Brokers) Rules of 2008. In considering whether a person is 'fit and proper' under section 20 of the Financial Services Act 2007, the FSC Mauritius may, inter alia, have regard to his financial standing; his education, qualifications and experience; his ability to perform the relevant functions properly, efficiently, honestly and fairly; and his reputation, character, financial integrity and reliability. His competence, being one of these elements of the fit and proper requirements, is assessed with regard to the person's education, qualifications together with relevant experience. The commission, like the UK's Financial Conduct Authority, is fighting shy of designing courses or examinations.

There are 3 levels of competency: basic (denoting a familiarity with basic concepts); intermediate (a thorough understanding of fundamental concepts "and their application in the field of knowledge"); and advanced (a thorough understanding of advanced concepts "and their application in the field of knowledge"). Language this loose might be thought meaningless. Nevertheless, this is not intended to be an exhaustive list of acceptable qualifications, so the regulator obviously wants to see some 'levelling-up.'

Parts of the document that sets out the standards put some – but not much – flesh on these brittle bones. A type 1 'new representative' of a full-service investment dealer, for example, must have an 'advanced knowledge' (this phrase is still not explained) of: the general principles of securities; securities products; the general principles of fund management and fund management products; and the regulatory set-up for securities-related activities in Mauritius.

"Like Weimar, this set of standards contains its own self-destruct mechanism"

Like the Weimar constitution's article 48, however, this set of standards contains its own self-destruct mechanism. Standard 4.6 states: "In the event that a person does not hold the minimum qualification or other comparable qualification, the commission may consider, on a case by case basis, whether the person has sufficient relevant experience to demonstrate the required competency level." The only possible explanation for this must be the fact that on small islands the appliance of even-handed justice breaks down when its target is a member of one of the interlinked ruling families, or a faithful retainer thereof.

MAURITIAN ABS NOT IN EVIDENCE

The standards do not mention the existence of British-style 'accredited bodies' such as the Chartered Insurance Institute. (The others in the UK are the CFA Society of the UK; the Chartered Institute for Securities and Investment (CISI); the Chartered Institute of Bankers in Scotland (CIOBS); the Chartered Insurance Institute (CII); the Institute of Chartered Accountants in England and Wales (ICAEW); the Institute of Financial Planning (IFP); the Institute of Financial Services (IFS); and the Pensions Management Institute.) They do, however, imply at 4.8 that the Mauritius Qualifications Authority has a monopoly on approval for any professional body (perhaps one of the British ones, many of which have international memberships) that wishes to run courses. The only other type of thing or

person who receives overt approval for this activity in 4.8 is "an officer or employee of the licensee [firm] who possesses the relevant qualification and experience to conduct the training."

CPD

Mauritius' mandatory structured CPD hours per annum are as follows: 10 hours for insurance salespersons, insurance agents, insurance brokers and their 'new broking staff', the newly-licensed reinsurance brokers and their 'new broking staff' and money-laundering reporting officers (MLROs) and 'alternate MLROs' (qualified to fill in when the MLROs are on holiday) appointed by licensees as from 1 January 2015; 15 hours for the new category of collective investment scheme manager; 'new representatives' of investment dealers (full service dealers types 1, 2 and 3, brokers types 1 and 2 and discount brokers type 1) licensed by the FSC Mauritius as from 1 January 2015 and for 'restricted licensed' and 'unrestricted licensed' categories of the same 'new representatives' of investment dealers. No mandatory time equals the UK's universal figure of 35 hours. The structure as a whole, however, is unmistakably based on the UK's. ■

SINGAPORE: A NEW BANKING ACT FOR A NEW ERA

Singapore's regulator is proposing to influence the government to give it more powers in a new bill.

The Monetary Authority of Singapore claims that it "is amending the *Banking Act* to strengthen its supervisory oversight over banks and to codify MAS' current supervisory expectations and practices." This eye-catching claim on the part of the regulator to be a legislative body is belied later in the text of the relevant consultative document, however. At the back of the document is a draft of the Banking (Amendment) Bill which clearly states: "Be it enacted by the President with the advice and consent of the Parliament of Singapore..."

Having got off on a rather farcical footing, the MAS lists the new powers that it would like. These are:

- the power to require any bank incorporated outside the island republic to be incorporated within it also;
- the imposition of debt ratio requirements;
- the imposition of minimum liquid assets or liquidity coverage ratios on banks;
- the discretion to prohibit (or render null or restrict) transactions with related persons that are detrimental to depositors' interests;
- the discretion to remove directors if they are not 'fit and proper';
- the ability to require banks to notify it as soon as they become aware of any material information that may negatively affect the fitness and propriety of any officer whose appointment the regulator previously approved;
- the power to penalise banks that fail to take reasonable care to ensure that the information they give it is accurate; and
- the power to declare bank holidays.

The MAS will formalise somebody's (it does not say whose - perhaps it means its own) expectation that banks will keep up adequate risk management systems and controls. It will consult interested parties about regulations to set out the risk management requirements in due course.

"The MAS wants to be able to penalise auditors for failing to discharge their statutory duties"

The regulator also wants a 'safe harbour provision' to protect external auditors from liability arising from disclosure, in good faith, of confidential information provided to it. It does, however, want to be able to penalise auditors for their failure to discharge their statutory duties as set out in the bill. It also wants to be able to direct a bank to remove external auditors who have not performed their statutory duties to its satisfaction.

Today, the MAS requires every bank to seek its approval whenever it wants to open a new place of business or change the location of its existing place of business at which it conducts any type of banking business. The MAS wants to be able to require banks to seek approval for places of business at which they conduct certain non-banking activities (e.g. money-changing and remittance business).

The bill, in its 'white paper' form, proposes to repeal the existing law that makes bank directors jointly and severally liable for their banks' losses arising from unsecured credit facilities. ■

A NOTE TO ALL RELATIONSHIP MANAGERS FROM THE EDITOR

Chris Hamblin
+44 207 148 0188
chris.hamblin@clearviewpublishing.com

How is compliance affecting your work?
This publication would like to know. RMs often have to deal with many conflicting business imperatives and these are likely to become more challenging still in the next year. My question, therefore, is this: what are your most important regulatory concerns and fears? I would like to hear from you in total confidence, with anonymity secured.

HONG KONG PROPOSES SWINGEING NEW REGULATORY POWERS IN THE NAME OF STABILITY

The Hong Kong Monetary Authority, the Securities and Futures Commission and the Insurance Authority might have sweeping new powers to allocate resources in the event of a financial meltdown, according to a consultative paper that the government has just released.

Hong Kong's Government and its financial regulators are asking interested parties for a second time about the issues involved in the establishment of a 'resolution regime' for financial institutions. This includes 'financial market infrastructures,' otherwise known as exchanges. The consultation period will be three months long.

The first stage of public consultation took place between January and April last year. During this period, the Government and financial regulators met Legislative Council members, trade bodies and professional associations, and received more than 30 submissions by the end of the consultation period. An overwhelming majority of respondents backed the idea of a resolution regime in Hong Kong.

This second stage of consultation seeks views on specific aspects of the regime including: further details of the resolution options and powers proposed in the first consultation paper; the 'governance arrangements' (especially the ones that are to govern 'resolution authorities'); and safeguards that might include a compensation mechanism that promises that no creditor will be worse off than in liquidation.

There may be a need to carry out a third, shorter consultative exercise later this year. It is not inconceivable that a bill will be on the stocks by the end of the year.

ENTER THE FSB

The impetus for the reforms comes from the Financial Stability Board, a successor body to the shadowy Financial Stability Forum whose guidance in the run-up to the financial meltdown of 2008 was not of the best. Jurisdictions, the FSB says, should evolve processes for recovery and resolution planning. Its latest paper on the subject of crisis resolution, published in 2011, calls for clear, transparent and enforceable set-off rights, contractual netting agreements, collateralisation agreements and (most importantly for wealth managers) client asset segregation.

Client assets, it says, are typically:

- money held on behalf of or owed to a client by a firm that is classified as "client money" under applicable national law;
- financial instruments or other assets held for or on behalf of a client;
- client collateral, i.e. assets received from a client and held by a firm for or on behalf of the client to secure an obligation of the client (other than under a title transfer transaction, see paragraph 3.2 (iii)); and
- assets and other (contractual) rights arising from transactions entered into by a firm on behalf of a client (for example, mark-to-market accruals arising from the change in value of futures and options positions).

Interestingly, the FSB does not include the following:

- deposits held by banks, except in the case of deposits held by a firm with a bank that constitute 'customer funds' under national law and are labelled as such;
- assets held by an insurer or policyholder, or claims and rights in connection with insurance business; and
- assets delivered in a full-title transfer transaction, such as securities lending transactions, repurchase agreements or reverse repurchase agreements, "where neither the client nor clients collectively retain proprietary or similar rights to the assets."

Another stand-out section in the document is no 7.4, which says: "National laws and regulations should not discriminate against creditors on the basis of their nationality, the location of their claim or the jurisdiction where it is payable." We wish the FSB good luck when it tries to enforce that point.

WHAT POWERS SHOULD RESOLUTION AUTHORITIES HAVE?

FSB section 3.2 lists a broad range of resolution powers for the authorities. They should be able to do the following at an afflicted firm:

- Remove and replace the senior managers and directors and recover monies from responsible persons, including claw-back of variable remuneration.
- Appoint an administrator to take control of and manage the affected firm with the objective of restoring it, or parts of it, to viability.
- Operate it, wielding powers to 'terminate contracts' (which might be the FSB's phrase for making them null and void), purchase or sell assets and write off debt.
- Ensure the continuity of essential services and functions by requiring other companies in the same group to continue to provide essential services to the entity.
- Override the rights of shareholders.
- Transfer or sell assets and liabilities, legal rights and obligations, including deposit liabilities and ownership in shares, to a solvent third party. (Some say that this is the whole point of having banking crises, as they are always likely to lead to a bonanza for the huge, 'in the know', policially connected financial institutions that cluster around the world's most powerful central banks.) The money could go to a newly established bridge institution.
- Establish a separate asset management vehicle and transfer non-performing loans or assets that are difficult to value to it.
- Carry out a 'bail-in,' defined by the *Financial Times* as 'the ability to impose losses on bondholders while ensuring the critical parts of the bank can keep running.'
- Temporarily stay the exercise of early termination rights.
- Impose a moratorium of payments to unsecured creditors and customers (excluding central counterparties) and put the claims of creditors on ice for a while.
- Effect the closure and orderly winding-up of a failing firm with timely payout or transfer of insured deposits and prompt access (perhaps within seven days) to transaction accounts and to segregated client funds.

WHAT POWERS SHOULD GO TO WHOM IN HONG KONG?

The reason why the Government thinks that there might be another consultative paper after this one is that the nations of today tend

to march in lock-step behind the international institutions that the major banks set up at the end of the Second World War - the Bank for International Settlements, IOSCO and so on - and one of these might have to reach another set of decisions before Hong Kong can be happy that it has received a full set of instructions to obey.

Neglecting this for a moment, then, the paper refers to its predecessor which set out two types of resolution regime. The first suggestion was for each of the sectoral regulators (the HKMA, the SFC and the IA) becoming the resolution authorities for financial institutions under their respective purviews. The second was to set up a stand-alone cross-sector resolution authority.

Respondents backed the first proposal, partly out of a desire to suck up to their existing regulators and partly to comply with the maxim "better the Devil you know than the Devil you don't." ■

GIBRALTAR'S PROPOSALS FOR NEW REGULATORY LEGISLATION AND ALL-IN-ONE RULEBOOK

The whole of Gibraltar's financial services legislation is being reviewed and its regulator, the Financial Services Commission, is looking at ideas for new guidelines. Chris Hamblin of Compliance Matters has been talking to some compliance officers on the spot.

The legislation appears to be mainly consolidatory, the government publishing a histogram in its publicity PDF that shows the mounting annual number of 'statutory provisions' (presumably including secondary legislation, which itself includes regulations) rising bumpily from 2 in 1987 to 28 in 1998, staying fairly static till 2003, then rising steeply through the 30 barrier to reach 60 in 2009, with a further steady rise to 90 in 2014.

AN UNWIELDY REGIME

The government therefore thinks that the financial services regime is now too unwieldy, too hard to understand (or 'navigate', to use its own word), too inconsistent between sectors (although when modern regulation was set up in the 1980s no regulator in either the UK or Gibraltar - or probably on Earth - had the slightest desire to promote consistency between them, seeing them as very different businesses), and not giving enough power to the regulators.

One compliance officer told *Compliance Matters*: "If you look at the FSC website, there are guidance notes, guidelines, newsletters put out by the FSC. You have to keep looking for different bits in different places, so it's not easily accessible. They also put out new things on their Twitter feed." The government is making a massive effort to consolidate this.

E PLURIBUS UNUM

The result will be a codifying Financial and Professional Services Bill, a universal rulebook or 'handbook' of regulation, a financial services ombudsman along the lines of that of the UK, a new appeals body to make the system look more just to the uninitiated, and other scraps of legislation here and there. The current 23 Acts - including the *Supervisory Acts* - will be gathered into one and 63 regulations will go into the 'handbook' which, one suspects, no human hand will be able to lift. The FSC has already begun to restructure itself. Whether it will cease to be an 'elephant's graveyard' for moribund British regulators remains to be seen.

Gibraltar is home to banks, e-Money Institutions, investment firms, payment service firms, insurance companies (general, including insurance-linked securities), occupational pension schemes, life offices, bureaux de change, reinsurance companies, a stock exchange, insurance intermediaries, trustee firms, insurance managers, company managers, alternative investment fund managers, auditors, experienced investor funds, insolvency practitioners and collective investment schemes.

A VAGUE CONSULTATIVE TIMETABLE

The colonial government and the regulator have not begun the inevitable consultative exercise yet. In view of the mountainous nature of the task they are not even promising that it will occur this year.

A tentative timetable, however, has been published for some things. Sometime in the first half of the year (before June, according to its forecast) the government says that it wants to consult interested parties about the main points that the eventual bill ought to have. It also proposes to ask the public about arrangements for ombudsman activity and 'compensation' - a word it is presumably not using to mean executive pay - before June. It expects the Financial Services Ombudsman to come into being in mid-to-late 2015. A more in-depth consultative process about the bill, including this time a discussion of the handbook and 'implementing legislation', will then take place. Then, in 2016, will come the second 'handbook consultation' and the handbook will come into force, along with the new law. Although regulatory experts from other jurisdictions might view this timetable as too optimistic, the FSC has a good reputation among compliance officers for sticking to its deadlines when consulting people.

The government seems concerned about the fact that these dates do not include the timetable for all of the European Union directives that will come into effect during the lifetime of the reform programme. Why this matters to the government in the context of this legislative project is a mystery; perhaps (although it does not say this) it expects some of the firms under its aegis to start obeying such EU legislation before it is enshrined in Gibraltar's new law and/or rulebook. Whatever the reason, it intends to set out the EU's legislative timetable in various consultative exercises to follow, perhaps thinking that the EU's own consultative processes are inadequate and require Gibraltarian support.

On the subject of ombudsman-related reforms, it appears that respondents will not have much of a say. The European Union has gone there first, passing an Alternative Dispute Resolution Directive in 2013. As for the reforms regarding 'compensation', these are to follow the Deposit Guarantee Scheme Directive of 2014.

CONFESSIONS?

In its proposals for legislative reform, the government seems to make a couple of stunning confessions: "By virtue of the new Act and handbook, firms and individuals will experience a risk-based approach to authorisation, supervision and enforcement. There will be clarity in terms of the FSC's expectations for firms and individuals, and transparency of decision making. The plans set out in this paper will also assist the FSC in delivering a more proportionate and outcomes focused approach to supervision."

This wording strongly suggests that British-style 'risk-based' regulation has yet to come to Gibraltar and, moreover, that the regulator is unclear about what it expects of firms and individuals when it deals with them. In fact, according to another Gibraltarian compliance officer: "In any dealings I have ever had with them, they've taken a risk-based approach. This is the way they've been doing things for years. The regulatory visits they go on and the documentation they send out are all done on a risk-based approach. I agree that they are making themselves look terrible by saying this, but I think they're [really] saying that they want to put it in legal writing for the first time." As for the admission about a lack of transparency: "It's the same here. They certainly are taking a transparent approach to firms and individuals, it's just a bit fragmented. There are no guidance notes on certain minor things. I think they're just documenting [this approach for the first time.]"

However, as for 'transparency' in decision-making, i.e. the public laying-bare of the process and rationale behind every decision, the Gibraltar FSC is unlikely to become the first regulator in the world to achieve a thing that has eluded all others. ■

ESMA'S MARKET RULES – THE DETAILS

The European Securities and Markets Authority has translated the provisions of MiFID II/MiFIR into practical rules for regulators and practitioners to follow.

The European Securities and Markets Authority has translated the provisions of the Markets in Financial Instruments Directive and its accompanying regulation into practical rules for regulators and practitioners to follow. The aim is to make secondary markets fair, 'transparent' and safe for investors who are buying investment products.

ESMA's "implementing rules on both secondary markets and investor protection issues" have taken account of a flurry of correspondence from interested parties. Some 'advice' that ESMA has formulated is now on its way to the European Commission - the nearest thing that the European Union has to an executive branch - to use when it prepares some delegated legislation, while ESMA's 'technical standards' (draft rules) are open for a second round of consultation.

MiFID II is to include most financial instruments, trading venues and techniques. MiFID II and the accompanying regulation MiFIR will, according to their authors, introduce changes to the functioning of secondary markets, including transparency requirements for a broad range of asset classes; the obligation to trade derivatives on trading venues; requirements for algorithmic and high-frequency-trading and new supervisory tools for commodity derivatives.

ESMA's main proposals in this round of rule-making are:

- an increase in 'trade transparency' for non-equity instruments, in particular bonds, derivatives, structured finance products and emission allowances;
- a trading obligation for shares and a double volume cap mechanism for shares and equity-like instruments - a major change to the EU's trading policy;
- an obligation to trade derivatives 'on MiFID venues' (regulated markets, multilateral trading facilities or organised trading facilities) only, in line with the wishes of the 'Group of 20' (actually only 19) of the world's most industrialised nations, whose opinions are evidently worth more to the EU than those of the next 20;
- newly introduced position limits and reporting requirements for commodity derivatives;
- rules governing high-frequency trading, imposing a strict set of organisational requirements on investment firms and trading venues;
- provisions regulating access to central counterparties, trading venues and benchmarks, designed to increase competition in the European Union; and
- requirements for a consolidated tape of trading data, with rules for tape-providers, reporting, publication and the sale of data.

MIFID II TO IMPROVE INVESTOR PROTECTION

ESMA wants the European Commission to take steps to further the protection of investors from sharp practice. Its main proposals in this regard include:

- more clarity about the circumstances in which portfolio managers can receive research from third parties;
- more clarity about the circumstances under which 'inducements' meet the 'quality enhancement requirement' for the provision of advice;
- requirements for investment firms that manufacture and/or distribute financial instruments and structured deposits to have product governance arrangements in place in order to assess the robustness of their manufacture and/or distribution;
- requirements for firms to provide clients with the details of all costs and charges related to their investments, including cost aggregations, the timing of disclosure (ex-ante and ex-post); information to non-retail clients; the scope of firms subject to this obligation; information on the cumulative effect of costs on the return;
- organisational requirements for firms that provide investment advice independently; and
- specification of powers for ESMA and national regulators with regards to prohibiting or restricting the marketing and distribution of financial instruments.

MiFID II/MiFIR and their so-called implementing measures (defined by one Europhile website, *eup-network.de*, as "mandatory requirements in the form of regulations that come into force without further implementation into national laws") will start to apply on 3 January 2017. ■