

# bankinginsight

IDEAS FOR LEADERS  
JUNE 2014

PP 17327/05/2013(032407)

**HARMONISING  
PAYMENTS  
THROUGH SEPA**

**PERSONAL DATA  
PROTECTION  
AND IMPACT  
ON BANKS**

**EMBRACE  
THE MOBILE  
REVOLUTION**

**TOWARDS  
A CASHLESS  
MALAYSIA**



ISSN 2231-6267



A Publication of  
Institut Bank-Bank Malaysia  
Institute of Bankers Malaysia  
35890 P



**BITCOINS:  
AYE OR NAY?**

**PREDICTING  
FINANCIAL  
CRIMES**






# CHARTERED BANKER

The gold standard in banking qualification.

The most prestigious professional qualification in banking, Chartered Banker is jointly awarded by the Institute of Bankers Malaysia and Chartered Institute of Bankers in Scotland, which is the oldest banking institute in the world. It is a badge that stands for a high standard in competency and integrity and is worn with great pride. Our online programme provides the flexibility that allows you to qualify as you work. Enrolment is ongoing, and the sooner you register, the faster you qualify. So what are you waiting for? Become a Chartered Banker today! For more information, visit us at [www.ibbm.org.my](http://www.ibbm.org.my).

**Chartered Banker**  
Leading financial professionalism

 **Institut Bank-Bank Malaysia**  
Institute of Bankers Malaysia

# CAPTURING THE E-NOVATION SPACE

**RAMPANT INNOVATION** and e-novation driven by rapid technological changes and social media channels are taking place globally in financial services, particularly in the payments space in developed markets.

In comparison, markets in Southeast Asia and Malaysia in general are still playing catch-up with developed jurisdictions where a diverse array of payment channels are phasing out the use of physical cash and traditional channels in favour of electronic payments. The payments system in Malaysia today comprises the ubiquitous cash, ATMs, cheques, telephone banking and credit cards, while the usage of debit cards, e-banking, e-money (through Touch n Go cards or smart cards, for example) and mobile banking has made inroads among consumers. However, two payment methods have yet to reach our shores - e-cash and the unsanctioned independent e-currency - bitcoins. However, it might pay off to enter the e-payments game a little later, since laggard markets could leapfrog to the front unhindered by costly legacy systems.

In this issue, *Banking Insight* takes a close look at the impact of innovations and e-novations in global payments systems. Perhaps one of the biggest repercussions of the relentless drive to embrace e-payments is the emergence of the cashless society. Not to be outdone, regulators in Malaysia too are encouraging more forms of electronic payments, for example by incentivising internet banking and discouraging cheque use through higher processing charges.

However, all stakeholders must bear in mind that financial service innovations ultimately must be undertaken for the benefit of users and consumers. Modernisation and reforms must serve the public interest, and suit the culture and environment into which they are introduced. E-novations should fulfill the goal of enlarging financial inclusion and uplifting social and public welfare. Innovations should also be timely. Given the current economic environment, is the crackdown on cheques really the way to go? Since most consumers from the lower-income strata are less tech-savvy, is it fair to penalise them for their preference for cheques as the de facto method of payment even as regulators and the government promote the e-banking agenda? Should consumers not avail themselves of the freedom

to choose the most appropriate and most convenient method of payment that suits their needs?

Security and legislation must also be modernised to keep up with innovations, in order to protect consumers and the public interest. Financial crimes are becoming rampant, moving from physical robbery to electronic fraud. *Banking Insight* looks at how financial institutions can better predict, detect and reduce financial crimes to manage this key area of risk. It is also critical to ramp up defenses for end-users of e-payments and e-banking, because the odds are currently stacked in favour of financial services providers. For example, electronic transfers can be disadvantageous for account payers in the event of a dispute, as the burden of proof for any unauthorised transfer is shifted to the account holder and the banker is no longer subject to the Bills of Exchange. This opens the door for the lowering of standards and bank negligence; thus, regulatory reform is urgently needed to keep abreast of innovations, and to insure security and confidence among users. Boosting assurance will be a catalyst for the adoption of e-payments among the masses, and this is aligned with the government agenda.

On the bright side, technology and innovations are enabling freedom of choice and access to alternative financial options – such as mobile banking and crowdfunding – for consumers and businesses which are excluded from conventional finance. In this issue, *Banking Insight* focuses on the crowdfunding phenomenon which is gaining traction among users which require easier access to funding and capital in an environment where lending and investment are becoming scarcer.

Looking forward, it is a certainty that innovations and e-novations will never cease in the banking and payments space. If Malaysia wants to be in the vanguard of financial services and e-payments in ASEAN, our industry and profession must be buttressed by a thirst for innovation, the judicious adoption of technologies, and the strategic stewardship of an enlightened and informed Malaysian banking leadership. \*

*Hope you have a fruitful read.*

**THE EDITOR**

**We want to hear** what you have to say on *Banking Insight*.

**Why not drop us a line now? e-mail:**  
publish@ibbm.org.my

**Visit us online at our new website**  
www.ibbm.org.my

## THE COUNCIL OF IBBM

### CHAIRMAN

Tan Sri Azman Hashim, FIBM  
*Chairman*  
*AmbInvestment Bank Berhad*

### VICE CHAIRMAN

Datuk Abdul Farid Alias,  
*Group President & Chief Executive Officer,*  
*Malayan Banking Berhad*

### MEMBERS

Mr. Donald Joshua Jaganathan, MIBM  
*Assistant Governor*  
*Bank Negara Malaysia*

Tan Sri Dato' Sri Tay Ah Lek, FIBM  
*Managing Director*  
*Public Bank Berhad*

Datuk Mohamed Azmi Mahmood, FIBM  
*Deputy Group Managing Director,*  
*AMMB Holdings Berhad*

Dato' Zulkiflee Abbas Abdul Hamid  
*Managing Director / Chief Executive Officer*  
*Affin Bank Berhad*

Mr. Jeffrey Chew Sun Teong  
*Chief Executive Officer / Director*  
*OCBC Bank (Malaysia) Berhad*

Mr. Wong Kim Choong  
*Chief Executive Officer*  
*United Overseas Bank (Malaysia) Berhad*

Mr. Kung Beng Hong, FIBM  
*Director*  
*Alliance Financial Group Berhad*

Mr. Tan Kong Khoon  
*Group Managing Director / Chief Executive,*  
*Hong Leong Bank Berhad*

Datuk Mohd Najib Hj. Abdullah  
*Group Managing Director / Chief Executive*  
*Officer, MIDF Amanah Investment Bank*  
*Berhad*

## EDITORIAL ADVISORY PANEL

### Chairman

Dr. Raja Lope Raja Shahrome, FIBM  
*Director*  
*OCBC Bank (Malaysia) Berhad*

### Panel Members

Dato' Dr. R Thillainathan, FIBM  
*Independent Non-Executive Director*  
*Genting Berhad*

Mr. Philip T N Koh  
*Senior Partner*  
*Mah-Kamariyah & Philip Koh*

Datuk Khairil Anuar Abdullah, FIBM  
*Chairman*  
*Pantai Holdings Berhad*

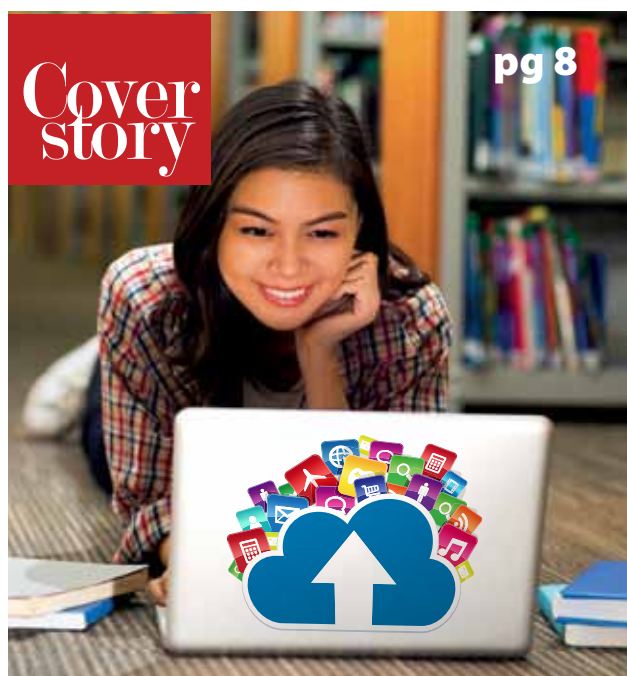
Professor Dr. Tan Hui Boon  
*Nottingham University Business School*  
*The University of Nottingham Malaysia*  
*Campus*

Dr. Cheong Kee Cheok  
*Senior Research Fellow, Faculty of Economics*  
*University of Malaya*

Dr. Bala Shanmugam  
*Finance Consultant*

### Technical Editor

Dr. Cheong Kee Cheok



**Editor** | Ms Chow Oi Li

**Writers** | Nazatul Izma, Jessica Furseth,  
Preetha Nadarajah, Anna Perry, Jessica Ree

### Publisher

Institut Bank-Bank Malaysia (35880-P),  
Wisma IBI, 5 Jalan Semantan, Damansara Heights  
50490 Kuala Lumpur  
Tel: +603-2095 6833, Fax: +603-2095 2322  
Email: [publish@ibbm.org.my](mailto:publish@ibbm.org.my)

### Publishing Consultant

Executive Mode Sdn Bhd (317453-P),  
Tel: +603-7118 3200, Fax: +603-7118 3220  
Email: [executivemode@executivemode.com.my](mailto:executivemode@executivemode.com.my)

### Printer

Percetakan Lai Sdn Bhd  
No.1, Persiaran 2/118C,  
Kawasan Perindustrian Desa Tun Razak,  
Cheras, 56000 Kuala Lumpur  
Tel: +603-9173 1111 Fax: +603-9173 1969

The views expressed in this magazine are not necessarily those of IBBM or its Council. Contributions including letters to the Editor and comments on articles appearing in the magazine are welcome and should be sent to the Editor. All materials without prejudice appearing in *Banking Insight* are copyright and cannot be reproduced in whole or in part without written permission from IBBM.

**Note:** All information provided in this publication is correct at the time of printing.

### BRANCHES

#### IBBM Penang Branch

Suite 4-02,  
Bangunan Sri Weld,  
3A Pengkalan Weld,  
10300 Penang  
Tel: (604) 2612619,  
Fax: (604) 2625825  
Email:  
[penang@ibbm.org.my](mailto:penang@ibbm.org.my)

# Contents

## June 2014

### Prospects

- 06** Insights
- 08** Towards a Cashless Malaysia
- 12** Going Cashless

*As the world tries to go cashless, banks are facing steep competition from innovative technology groups to offer attractive options to consumers. The key may well be to link payments to everyone's favourite gadget: the mobile phone.*

- 16** Leading the World of Cashless: Royal Bank of Canada
- 20** Harmonising Payments Through SEPA
- 24** Bitcoins: Aye or Nay?
- 30** Policing Bitcoin
- 32** Crowdfunding Takes Off

### Governance

- 36** Personal Data Protection and Impact on Banks
- 40** Data Protection and Banks in the ASEAN Region
- 46** BBVA: Leading in Personal Data Protection

### Thought Leadership

- 50** Reform to Perform
- 54** Embrace the Mobile Revolution

### Management

- 58** Predicting Financial Crimes

### Technical

- 62** Control - Key to Cybersecurity
- 64** Aiming for Zero Downtime



## PAYMENTS' HOT SPOTS



**GLOBAL NON-CASH PAYMENTS VOLUMES** topped 333 billion transactions in 2012 after transactions grew by 8.8% in 2011, according to the 'World Payments Report 2013' by Capgemini and RBS.

Central Europe, the Middle East, Africa (CEMEA) and Emerging Asia are leading the charge with growth in transaction volumes of more than 20%, while Latin America recorded growth of 14.4%. Growth in these emerging economies outpaced that of the developed markets of North America, Europe and Mature Asia, which recorded single digit growth rates, though mature markets still account for more than two-thirds of global non-cash transaction volumes with a 76.9% share. Forecasts show, however, that for all the growth in the surging economies of Asia and Latin America, it will still take at least 10 years for emerging markets to overtake mature markets in transaction volumes.

"In the developing markets, mobile payments are giving more people access to financial transactions, while customer-centric innovation has helped prepaid cards and virtual currency gain traction in the more developed markets," said Kevin Brown, Managing Director, Global Head of Transaction Services, RBS International Banking.

Debit and credit cards continue to be the most popular non-cash payment instruments, ahead of e- and m-payments, according to Capgemini. \*

## GOOD GROWTH PROGNOSIS FOR EAST ASIAN ECONOMIES

**DEVELOPING COUNTRIES IN THE EAST ASIA PACIFIC** region will see stable economic growth this year, bolstered by a recovery in high-income economies and the market's modest response so far to the Federal Reserve's tapering of its quantitative easing, according to the 'East Asia Pacific Economic Update' released recently by the World Bank.

Developing East Asia will grow by 7.1% this year, largely unchanged from 2013. As a result, East Asia remains the fastest growing region in the world, despite a slowdown from the average growth rate of 8.0% from 2009 to 2013. In China, growth will ease slightly, to 7.6% this year from 7.7% in 2013. Excluding China, the developing countries in the region will grow by 5.0%, slightly down from 5.2% last year.

"East Asia Pacific has served as the world's main growth engine since the global financial crisis," said Axel van Trotsenburg, World Bank East Asia and Pacific Regional Vice-President. "Stronger global growth this year will help the region expand at a relatively steady pace while adjusting to tighter global financial conditions."

Larger Southeast Asian economies, such as Indonesia and Thailand, will face tougher global financial conditions and higher levels of household debt. Malaysia's growth will accelerate modestly, to 4.9% in 2014. Its exports will increase, but

**Malaysia's growth will accelerate modestly, to 4.9% in 2014. Its exports will increase, but higher debt servicing costs and ongoing fiscal consolidation will weigh on domestic demand.**

higher debt servicing costs and ongoing fiscal consolidation will weigh on domestic demand. In the Philippines, growth could slow to 6.6%, but accelerating reconstruction spending would offset the drag on consumption from the effects of natural disasters in 2013.

The smaller economies are expected to grow steadily, but face overheating risks that could require further monetary tightening. \*





## MORE PAIN AHEAD FOR UK BANKS

**FURTHER PAIN IS AHEAD FOR UK** banks as the sector struggles to reconcile the conflicting demands of investors, customers, regulators and government, according to a KPMG report which analyses the 2013 results of the UK's five largest banks.

Headline figures show that total assets have fallen 25% over five years to £5.2tn, capital reserves have been boosted by £93bn since 2008 and the banks have faced a £28.5bn bill for litigation, fines and customer redress.

KPMG's report, 'Reinvention of UK Banking', highlights that as the cost of remediation – both in financial and resource terms – continues to dominate results presentations, banks face an uphill battle as they try to radically transform in a timeframe that is acceptable to all stakeholders.

Banks also face the challenge of lower returns on equity – currently below banks' cost of capital – which are not only constraining banks' ability to offer more, and better priced, products to customers but could also impede their ability to attract capital.

KPMG's report highlights that 80% of the 2013 profits of the five largest UK banks went towards remediation costs, hindering investment in the future, particularly in 'mission critical' technology needed to replace archaic legacy systems. \*



### FINTECH INVESTMENT BOOM

**GLOBAL INVESTMENT IN FINANCIAL TECHNOLOGY** (fintech) ventures has more than tripled from USD928 million in 2008 to USD2.97bn in 2013 and, over the past three years, such investment increased at more than four times the rate of overall venture capital investment, according to a new report by Accenture entitled 'The Boom in Global Fintech Investment; A New Growth Opportunity for London'.

Although the US remains the dominant market for fintech investment, the fastest growing region is now the UK and Ireland (UKI). Deal volume, mostly related to London, has been growing at an annualised rate of 74% since 2008, compared with 27% globally and 13% in Silicon Valley.

During the same period, the value of fintech investment in UKI increased nearly eightfold to USD265 million in 2013. The annualised growth rate (51%) was nearly twice the global average (26%) and more than twice that of Silicon Valley (23%). As a result of the rapid growth in UKI, which accounts for more than half (53%) of all investment in Europe, London has emerged as the fintech capital of Europe, according to the study.

The growth of London's fintech cluster has been driven by its strength in financial services and a thriving tech sector that has enjoyed an entrepreneurial renaissance in recent years. Four of the world's ten biggest banks have either global headquarters or European headquarters situated in London. There are approximately 135,000 financial-services technology workers in the UK, according to the Accenture study. \*

# Towards a Cashless Malaysia

■ CHEAH KOK HOONG

The convergence of the four primary forces - mobility, social media, IT cloud models and data/information – is catalysing the digitisation of banking channels, and thus, the implementation of the true 'Cashless Society'. Where does Malaysia stand in its evolution towards becoming a cashless society?



**T**

oday, forces such as mobile, social media, information technology (IT) cloud models and information are converging in an innovative

nexus that is changing society and the behaviour of communities, as well as creating new business scenarios. According to Gartner research, this is a result of IT consumerisation and the ubiquity of connected smart devices.

The banking industry is no exception to this phenomenal trend. Many banks are adapting their service models to cater to their customers who are increasingly living a digital lifestyle. For instance, consumers nowadays are spending a lot more time with their mobile devices to find out what they want to purchase or subscribe to. After making online comparisons, their next step is to seal the transaction over a trusted payment channel, more likely via their own banking provider.

At the same time, the manner of transferring the value of money is increasingly being digitised with the impacts of the four forces of mobility, social media, IT cloud models and data/information.

The collision of these trends is catalysing the world to finally and truly realise an actual adoption of the long-time 'Cashless Society' concept - whereby the usage of physical payment methods such as cash and cheques diminish and give way to more cashless mediums such as debit and credit cards, online credit transfers, mobile payments, banking portals, digital wallets, cryptocurrencies and more.

### The Local State of 'Cashless'

With regards to the local scene, cashless payments account for 45% of the total values of consumer payments in Malaysia, according to the latest estimation from MasterCard Advisors' 'Cashless Journey' study in September 2013. This study was specifically

developed to measure the nation's progress in evolving consumers' payments from cash to cashless.

The same study suggested that Malaysia's cashless journey will be catalysed by emerging technologies like mobile acceptance solutions, which will fast track the traditional path that has typically been predicated based on the wired merchant acceptance infrastructure. At the same time, it is envisaged that new payment options and Near-Field Communication (NFC)-enabled solutions for parking and transit being rolled out in Malaysia will also help shift the cash share of total transaction volumes to cashless in the near future.



**Malaysia is currently** in the transitioning stage from cash to cashless.

Malaysia is currently in the transitioning stage from cash to cashless. An upward trajectory of cashless transactions is influenced by factors such as ease of access to financial services, uptake of cashless payment solutions by merchants, technology and infrastructure readiness, and macro-economic and cultural aspects.

Moreover, in 2013, Bank Negara Malaysia announced the reduction of fees to a mere 10 sen for all Interbank GIRO or IBG transactions that are performed online via Internet and mobile banking. The low online fee is aimed at incentivising the mass market to switch from costly physical payment methods to lower-cost alternatives. In a single brave stroke, the central bank decision demonstrated intent to spur the growth of cashless transactions.

For banks and many businesses in the financial sector, a cashless society will substantially lower their costs by removing the need to handle cash on a daily basis. Freed from the need to physically count, store or move the cash, almost all the related parties and institutions can also operate more safely, securely and accurately via the digital platforms that fundamentally facilitate the various cashless scenarios.

In combination, all of these factors will prove irresistible for all modern banks to invest not just into making analogue processes into digital, but also to innovatively create new processes, products and services to meet the demands of the cashless society.

### Technology Spurring the Cashless Journey

Despite the positive signs, Malaysia continues to face certain challenges in growing more cashless payment activities. Some of these challenges include a low rate of credit and debit card possession, and a relatively large percentage of informal business sectors that do not naturally fit into the default cashless transaction ecosystem. In addition, the absence of a proper regulatory and policy framework pose some risks in integrating new cashless mediums and models into the entire monetary landscape.

From a technology standpoint, developing a comprehensive digital strategy requires banks to envision the enablers to support the banking and payment modernisation roadmap based on a sustainable and agile strategy.

Banks can tap on the nexus of four forces to create new processes, products and services to serve consumers. As one of the best routes to market, mobile technology offers the real potential to significantly change the consumer-facing portion of banking. It reshapes the bank's channel mix with a compelling computing and service platform to engage with customers at a whole new, personal level.

Technology is indeed creating opportunities for banks to develop new revenue streams based on a cashless society, but it is imperative that building cashless payment channels does not become just another IT project. Banks' most successful digital cashless payment strategy must focus on anticipating and creating new customer needs in tandem with adapting to how retail is evolving. For example, how will people prefer to shop to ensure that they capitalise on the digital money opportunity?



**For banks and many businesses** in the financial sector, a cashless society will substantially lower their costs by removing the need to handle cash on a daily basis.

### GST Amplifies the Cashless Society Development

In tune with local developments, the impending Goods and Services Tax (GST) to be implemented by 1 April 2015 reinforces the market's and nation's move towards a truly cashless society as the imposition of GST requires businesses to capture all their sales accurately. Thus, it is a key enabler to facilitate the ease of making payments electronically via the proper payment infrastructure.

According to Bank Negara Malaysia, today 1.6 billion financial transactions are carried out via electronic means, double the amount in 2006. The target is to increase the number of electronic payments per capita from 56 in 2012, to 200 by 2020. Achieving this target would bring Malaysia closer to reaping annual savings of up to 1% of GDP – which is the estimated amount that the economy would achieve by shifting from being predominantly paper-based to more electronic-based payment systems.

The need to accelerate the migration is even more important now as Malaysia transitions towards a value-added and high-income economy.

### **Moving Forward**

Today's financial systems and payment channels are indeed the result of centuries of innovation. However, with improved access to technologies and information, consumers have become more demanding in terms of requiring all sorts of new digital channel options for real-time electronic transactions. This forces banks to continually provide innovative banking, payments and commerce solutions to consumers that can be used on any device, across any platform.

Visualising the banks of the future and asking the right questions are instrumental for banks to uncover the opportunities to capitalise on cashless mediums, complement existing models, create new revenue streams and strengthen presence in consumers' wallet share.

The movement towards a more cashless society is proceeding incrementally. It is an exciting time for consumers as they will be presented with a myriad of digital banking and payment choices, in addition to cash. All available evidence and trends indicate that it is imperative for banks to play an active role in shaping the future of the 'cashless society', or risk being left behind. \*

■ Cheah Kok Hoong is Group Chief Executive Officer and Director for Hitachi Sunway Information Systems Sdn Bhd (HSIS). In this role, Cheah is responsible for the entire HSIS operations in Southeast Asia, leading the growth and support of three core HSIS business lines - enterprise-level business applications, infrastructure and managed services, and engineered solutions. Cheah is also the Chief Information Officer (CIO) of the Sunway Group, and Deputy Chairman for both the National ICT Association of Malaysia (PIKOM) and Outsourcing Malaysia.



# Going Cashless

■ JESSICA FURSETH



**AS THE WORLD TRIES TO GO CASHLESS,** BANKS ARE FACING STEEP COMPETITION FROM INNOVATIVE TECHNOLOGY GROUPS TO OFFER ATTRACTIVE OPTIONS TO CONSUMERS. THE KEY MAY WELL BE TO LINK PAYMENTS TO EVERYONE'S FAVOURITE GADGET: THE MOBILE PHONE.

International Settlements, compared to 9% in the Eurozone.

But this is hardly status quo across the globe. The world is mostly cashless when it comes to moving large sums of money, but cash is still king for 85% of the smaller retail transactions. Money in the hand may be handy for picking up coffee, newspapers, or paying for a taxi, but the prevalence of cash costs society an estimated 0.5% to 1.5% of gross domestic product (GDP). This is a lot, especially considering consumer payments make up just 11% of the value of payments around the globe.

Banks and payment groups are happy to see cash become history, as they make money on each electronic transaction. Government intent and regulatory incentives have, however, proven vital to shaping a nation's attitude to electronic payments. Swedish regulations now restrict retailers from passing on credit card payment fees to customers, hence encouraging card use among consumers. The opposite effect is happening in certain US states, where lawmakers allow retailers to charge customers for using cards. The Irish government is currently planning a major campaign to double the number of debit card and other electronic



payments and transfers, while this year also sees the introduction of the Single Euro Payments Area (SEPA). While, most cashless initiatives are national or corporate, SEPA will create a common set of payment standards to make the process simpler and quicker across the entire Eurozone.

**T**he first European country to introduce banknotes was Sweden in 1661. True to its pioneering spirit, it is fitting that Sweden should be among the world's first countries to do away with cash altogether. Today, most Swedish city buses do not take cash, accepting only prepaid tickets. An increasing number of businesses only take cards, while the majority of branches at Nordea Bank and Swedbank no longer handle cash. As Swedes are losing the cash habit, even houses of worship are installing card readers to take donations. Bills and coins represent just 3% of Sweden's economy, according to the Bank for

India, Indonesia, Russia and the United Arab Emirates are all below 30% cashless, needing innovation from both the financial sector and governments in order to trigger the necessary shift.

For banks and financial institutions, allowing people to move funds via the telephone and internet is just the first step. Next is enabling PIN-free payments for low-value purchases, first by using payment cards, and now increasingly also by using mobile handsets. When it comes to transferring funds directly between individuals, technology companies have made major inroads, sometimes circumventing banks altogether. In the Western world, this usually means moving funds using basic information such as e-mail addresses or even social media. Meanwhile, in the developing world, mobile phone companies have stepped up and created innovative payment systems in areas where conventional bank branches are few and far between. On a basic level, all of these solutions require a steady supply of electricity, data lines, computers and readers for credit cards or mobile phones.

## How to Accelerate the Cashless Journey

When convenient payment systems are in place, most people are happy to pay for goods and services electronically; after all, it is easier to carry a card or a mobile device around rather than piles of cash. After researching 33 countries across five regions, the MasterCard 2013 'Cashless Journey' study found that Belgium, France, Canada and the UK are now over 90% cashless, based on the share of non-cash payments of the total value of consumer payments. This puts them close to the finishing line, but moving any closer will require determination and innovation. For these countries, the current systems cannot quite replace cash for that last 10% of economic activity: tipping couriers, lending to a friend, or throwing change into a charity bucket.

"Many markets have made real progress on their journeys by establishing basic infrastructure over long periods of time. Affordable and broadly available financial products, a vibrant and competitive merchant marketplace, a transparent and

productive business environment - all of these basics are strongly correlated with progress in the cashless journey," said Hugh Thomas, Senior Managing Consultant at MasterCard's Global Payments Strategy Knowledge Centre.

Germany, Singapore, South Korea and the US are at a tipping point towards cashlessness, having moved most payments away from cash. Brazil, China, Malaysia and Spain are in a transitioning phase, where progress is rapid but cash still accounts for about half of all transactions. India, Indonesia, Russia and the United Arab Emirates are all below 30% cashless, needing innovation from both the financial sector and governments in order to trigger the necessary shift.

"Five years of rapid progress in Kenya and China have shown us that encouraging payment product innovation and strong government cash reduction leadership can dramatically

accelerate the cashless journey," said Thomas, adding that markets like Germany illustrate how markets can plateau despite having the infrastructure in place: "If specific consumer attitudes and behaviours towards cash usage are not well understood or accommodated, consumers may prevent the cashless journey's completion."

## The shadow economy

Can going cashless pre-empt traditional crimes? One interesting side-effect of the cashless society is how the number of bank robberies in Sweden are at the lowest since records began 30 years ago, and attacks on security transports are also down. Sweden has, however, seen a rise in electronic crime, with computerised fraud cases having increased sixfold in the past ten years, according to the Swedish National Council for Crime Prevention.

*"Cash is easy to hide from authorities, fuelling one of society's most damaging phenomena: the shadow economy."*

Generally though, the ability to weed out crime, fraud and corruption is an argument in favour of the cashless society. "Cash is easy to hide from authorities, fuelling one of society's most damaging phenomena: the shadow economy," said Prof. Dr. h.c.mult. Friedrich Schneider, Professor at Johannes Kepler University of Linz in Austria and author of Visa's 2013 report 'The Shadow Economy in Europe'. Defined as "the blurry area of commerce that includes legal activity hidden deliberately from public authorities", Schneider estimates the European shadow economy to be worth over

€2.1 trillion. This represents 18.5% of economic activity in the region. While heavy use of cash makes it easier to under-report earnings and avoid taxes, Schneider points out there is a psychological element: "Austerity programme extremes, such as slashed wages and pensions, budget cuts in healthcare and education, and rising unemployment, [mean] citizens feel left alone to deal with the consequences of the economic crisis. Hence, the step into the shadow economy is made with less remorse."

The report shows that putting better electronic payment facilities in place will still be helpful, as most people are honest and will be drawn to convenient methods. "Increasing electronic payments by an average of 10% annually for at least four consecutive years can shrink the size of the shadow economy by up to 5%," concluded Schneider.

Critics of the cashless society have pointed to its lack of privacy, as there would be no such thing as an untraceable transaction. There is also concern about the power it would award to financial corporations to monitor people's lives, not to mention how difficult it would be to keep a surprise under wraps if every gift showed up on the credit card receipt. David Wolman addressed this in his book 'The End of Money': "[There is a] distinction between what is anonymity and what is privacy. Even though everyone loves cash for the anonymity, it is not really something that goes along with our lives in a modern democracy." Speaking to 'Salon', Wolman deemed the desire for privacy to be a secondary concern, as complete cashlessness would make it easier to trace criminal activity.

Cashlessness would probably mean better services, added Wolman: "When we go cashless, people would wake up to this great flowering of payment options. We will be more demanding of banks and mobile services to lower their fees, and provide us with confident services. That is why PayPal was so successful: they finally convinced people you can do this securely. It is not perfect, but it is safe enough that people are game to go along with it."

### **The Financial Inclusion Challenge**

Financial inclusion has been a priority for the European Commission over the last three years, and several EU member countries have since changed regulations to encourage banks to offer basic accounts to people with previous debt problems or without credit histories. Another initiative is prepaid cards, originally introduced as a way to reach low-income consumers. Their popularity is however spreading: this year USD167bn is expected to be loaded onto prepaid cards, according to a study from Mercator Advisory Group.

Some of the most rapid progress towards cashlessness is found in Asian countries. South Korean tax authorities now offer a lump sum refund if credit card usage exceeds 20% of individual gross income. Consequently, card usage has risen from under 5% two decades ago, to over 65% today. China has made strides away from cash in recent years in part due to rapid urbanisation, as well as attractive government incentives for moving to electronic payments. Having said that, official incentives may not be enough if the public is not willing, as seems to be a factor in Japan and Taiwan. Extensive ATM networks with cheap cash withdrawal, and low rates of street crime mean there is little risk in carrying large amounts of cash. As a result, these countries have seen their journeys to cashlessness stall.

Surprisingly, there is no strong correlation between financial inclusion and people's attitudes to cash, even though it is the poorest who pay the most to move money. This was the conclusion from Tufts University's 2013 study 'The Cost of Cash in the United States'. "The lowest-income Americans paid the most in fees for cash access. This is an unsurprising finding, but it refutes the idea that cash is somehow better suited to low-income households," said Bhaskar Chakravorti, Senior Associate Dean for International Business and Finance at the Fletcher School at Tufts University. "The prices for cash-out transactions are systematically higher for the unbanked than for the typical consumer. Bringing these consumers into the financial system could improve the prices they face in the marketplace, provided the accounts they adopt do not offset gains with additional periodic fees, transaction fees and penalties."

Still, banks have to contend with the force of habit and inertia that lock in behaviours and expectations. Cash remains prevalent because everyone accepts it as a legitimate form of payment, adds Chakravorti, whereas "adopting a new payment interface, whether it involves a new interface for an existing account or a new set of hardware to acquire payments from familiar payment cards, entails new behaviours, risks or expectations that merchants and consumers are ill-equipped to assess."

## A Mobile Push

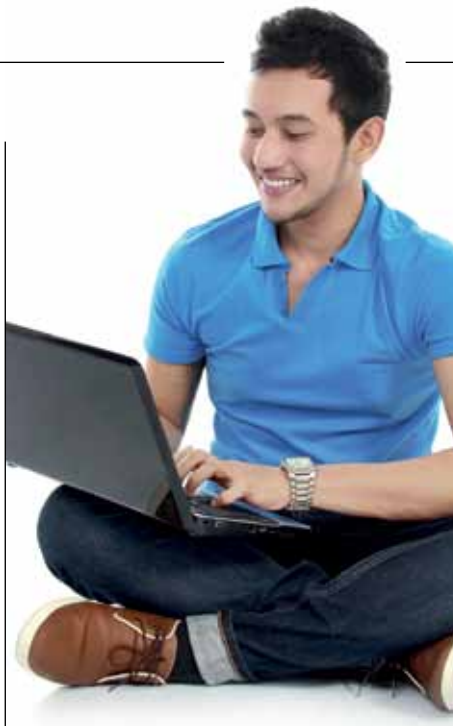
As banks are realising they need to make electronic payments very simple and convenient in order to tempt people to make the move, the key seems to be linking to people's favourite gadget: the mobile phone. Australia's CommBank now lets customers make payments by simply waving their handsets. The Near-Field Communications (NFC) system comes ready loaded on new Samsung phones, or customers can attach a NFC sticker to their existing handsets.

In 2013, mobile devices and connections grew to 7 billion worldwide, and smartphones accounted for 77% of that growth, according to research from Cisco Visual Networking. These devices now represent 21% of all devices. One in every two mobiles purchased in Southeast Asia is now a smartphone, according to market research agency GfK Asia; Indonesia leads the pack, with Thailand and Malaysia closely behind.

While smartphones are still few and far between in many developing countries, basic handsets are proving just as useful in the journey to cashlessness. Launched in 2007, Kenya's M-Pesa mobile payments network has become a viable alternative to banks for 17 million people in the country, or two-thirds of the adult population. Launched by Safaricom, funds can be added to M-Pesa by handing cash to one of the mobile group's 40,000 agents. Over USD10bn worth of transactions are moving through the system every year, paying for everything from groceries to school fees.

M-Pesa has become a success because traditional bank branches in the Kenyan countryside are sparse, and transferring money in the traditional manner is expensive. During the post-election violence in the country in 2008, many Kenyans regarded M-Pesa as a safer place to store their money as several banks were entangled in ethnic disputes. Studies have suggested a correlation between use of M-Pesa and increased household income, while the country has seen several business start-ups launch with a basis on the M-Pesa model.

ICICI Bank and Vodafone are in the



process of rolling out M-Pesa across India, where just 5% of villages have bank outlets. The scheme has also been launched in Afghanistan and Tanzania. Western Union, working with mobile operator MTN, has launched a similar scheme in 21 countries in Africa, Asia and the Middle East. However, many other countries find their budding mobile money schemes are being held up by regulators concerned with money-laundering and by opposition from banks worried about competition.

Even so, innovative alternatives to cash and standard money transfers are coming along thick and fast. Google partnered with MasterCard and telecoms operator Sprint to create Google Wallet, which lets users make one-tap payments using their mobiles. Spanish bank La Caixa has rolled out a network of contactless payment cards and shop terminals in Barcelona. Twitter founder Jack Dorsey partnered with Swedish start-up iZettle to create Square, a card reader that can be attached to the bottom of an iPhone to take payments. Barclays Bank in the UK has launched Pingit, where customers can send money to someone else with no information other than their phone number. BitCoin is a virtual currency that eschews the traditional financial system altogether.

## The Need for Innovation

There is a major market for simple ways to transfer money, and if banks do not step up, others will. In an effort to catch up with PayPal, last year American Express launched Serve, which has since copied PayPal's idea to let users pay each other via Facebook. Governments keen to move towards cashlessness need to be open to initiatives from both banks and technology companies, while also making sure regulation is in place to protect consumers' money in case an experimental system collapses. "When we talk of the War on Cash, there are really two separate battles," Samee Zafar, Director at financial consultancy Edgar Dunn & Company, said to 'Banking Technology'. "The war for mid- and high-value payments is already finished. People have moved from cash to credit and debit cards. The war still being fought is for low-value payments."

While the trend towards cashlessness is clear, it seems unlikely that the world will get rid of cash entirely, at least not any time soon. While visits to bank branches are dropping, people remain attached to the idea: Metro Bank, Virgin Money and Handelsbanken are all planning new branches this year. The technology exists to make almost any transaction electronically, but we are far away from a system that everyone agrees on - the one major advantage of cash. Last year, the Bank of England announced plans to start printing bank notes on plastic instead of paper, a more hygienic and durable material, in recognition of the continued importance of hard cash. The first note to go plastic will be the £5, replacing the 250 million notes in this denomination currently in circulation. Even though the UK is already 89% cashless, each £5 note lasts only about a year before it is worn out by frequent use.

Cash is still king; it will take a while before the reign of cash ends. \*

■ Jessica Furseth is a freelance journalist based in London.

CANADA HAS BECOME A WORLD LEADER IN THE MOVE TOWARDS CASHLESSNESS. ITS BIGGEST BANK, THE ROYAL BANK OF CANADA, HAS ATTRACTED ATTENTION WITH ITS GROUNDBREAKING NEW PAYMENT SYSTEM, ONE WHICH AIMS TO REPLACE THE WALLET ALTOGETHER.



As the world's payment method of choice moves from cash towards plastic, Canada is the country that has come the closest to total cashlessness. 90% of consumer payments in Canada now take place using electronic means, according to MasterCard's 2013 'Cashless Journey' study, and the country is the world leader in terms of having the necessary systems in place to move even further away from cash.

Widespread prevalence of credit and debit cards and a modern payment infrastructure system is one factor to Canada's progress. The successful transition from magnetic strips to EMV, the global security standard for chip card technology, is another. Near-Field Communication (NFC) technology lets people use their cards and now even their mobile handsets to make low-value purchases with a simple tap on a reader. "The increased adoption of electronic payments has propelled Canada to leapfrog other countries and secure a top spot as nearly cashless," said Betty DeVita, President of MasterCard Canada. "Canadians are comfortable with and prefer using other forms of payment, and have been at it for years."

At the centre of Canada's route to cashlessness is the Royal Bank of Canada (RBC), the country's largest bank by assets and market capitalisation. Founded in Canada in 1901, RBC now operates in 46 countries, servicing 15 million clients nationally, in the Caribbean and in the US. While the bank also provides wealth management, insurance, and investment banking, over half the bank's earnings come from personal and commercial banking. Listed on the Toronto Stock

Exchange, RBC makes almost two-thirds of its revenues in the Canadian home market.

## Cloud Pioneer

Last year RBC launched Secure Cloud, the country's first cloud-based mobile payments solution. Secure Cloud lets users pay for goods and services using their mobile devices, with their personal information kept safe in a remote data cloud. This is different from many other mobile payment systems, which often keep the data inside the device itself. With Secure Cloud, the data is encrypted during transmission, and decoded at the point of sale through partnerships with mobile services providers.

"We understand the importance of security to our clients and make safeguarding their personal information our highest priority," said Paul Gerics, Vice-President of Information Security at RBC. "We employ a diverse range of technologies and security mechanisms to help ensure the safety, confidentiality and integrity of our client's information and transactions."

Initially, Secure Cloud uses NFC technology, enabling customers to pay for small purchases by waving their phones over readers at shops that accept contactless payments. The system is however built for flexibility, anticipating technology standards to evolve. Offline transactions are already possible, and the collaborative system even has the ability to support payment methods used by RBC's competitors. Initially launched on Android smartphones, using NFC-enabled SIM cards on the Bell network, the bank plans to roll out Secure Cloud to work on all phones, with all carriers, all financial institutions, all card products, and with all merchants.

**90%**  
consumer  
payments in  
Canada takes  
place using  
electronic  
means.



# Leading *the World of* cashless

ROYAL BANK OF CANADA

RBC held its first Emerging Payments Merchant Forum in January this year, in an effort to engage with leading retailers to explore options for the future of contactless payments. RBC is also engaging consumers, merchants, network operators and its own employees to test new services, incorporating feedback before introducing new features to the general public. "We will not bring anything to market until we are confident that we have the very best solution, which meets the needs of our customers, merchants and all other partners," said Dave McKay, Group Head of Personal and Commercial Banking at RBC.

Industry observers are watching RBC's Secure Cloud system with interest, as this is one of the first major commercial launches of an NFC-based payment system. RBC's system basically stores customers' credit and debit cards virtually, in what is known as the RBC Wallet. Gift cards or loyalty cards can also be stored in the same place, and applied when relevant. Over 80% of Canadians have at least one store loyalty card, according to research from RBC and Shoppers Drug Mart.

### **Collaboration is Key**

Last year RBC also became the first bank in North America to offer person-to-person money transfers via Facebook. Using the RBC Canada app, customers can securely send money to others on the social network without sharing any personal or financial information. "Our social person-to-person solution provides our clients with the added simplicity, convenience and choice to bank in the manner in which they interact on a daily basis, with the security they expect from RBC," said McKay who explained this is likely to be used at first to pay friends for concert tickets or dinner.

The RBC Facebook payment system uses Canada's standardised electronic payment system, Interac. Previously, users needed the recipient's email address or mobile phone number to use Interac; however it is now enough to simply select the recipient on Facebook.



"Our social person-to-person solution provides our clients with the added simplicity, convenience and choice to bank in the manner in which they interact on a daily basis, with the security they expect from RBC."

**Dave McKay,**

Group Head of Personal and Commercial Banking at RBC

The recipient will be notified, and then directed to deposit the funds into their bank account of choice. RBC's new initiative is available on iPad and iPhone, with other platforms to follow this year. 9.4 million Canadians use Facebook on their mobile device on a daily basis.

Vital to RBC's success is its collaboration with other industry players, especially mobile operators. The Canadian government has been clear in its encouragement for banks to do this since its 2011 Payments System Review; this has resulted in a new set of guidelines to provide a common platform for the banking and credit union industry to develop mobile payments at point-of-sale in Canada. The idea is to encourage innovation and hence speed up the move towards cashless transactions at the lower end of the value chain, while also ensuring security is maintained as payment methods change. The guidelines set out how information should be exchanged among the parties in the transaction, including financial institutions, payment card companies, telecommunications companies and merchants.

### **Getting Consumer Buy-In**

Encouragement from government initiatives and attractive services from banks are two reasons explaining why Canada has come so far in its journey to cashlessness. The third reason is

arguably that its citizens are genuinely motivated to move away from cash, a factor that has held back other countries where the methods are in place, but a reluctance to stop using cash is hampering progress. A study conducted by Leger Marketing on behalf of PayPal Canada showed that 71% of Canadians are comfortable with never having to handle cash to make a purchase, while 25% of respondents already go more than a week without using cash. "The growth we are seeing in Canadians' eagerness to go cashless is significant," said Darrell MacMullin, Managing Director of PayPal Canada. MacMullin added that Canadians are beginning to understand that a digital wallet can be a safe way to move money. Separate studies show security is still the main concern as consumers consider whether to adopt mobile payment technology, meaning banks and technology providers have to work hard at convincing people the new methods are safe.

### **Online Banking Leader**

RBC has been offering a dedicated mobile banking app to customers since 2008. Earlier this year, RBC's online banking services were named the best in the country for the fourth year in a row. Canadian business analytics group Survisor considered features, functionality and service interaction at the country's 16 major banking institutions for the rankings, which

found the five biggest banks also occupied the top five spots.

“While the competition has closed the gap, RBC has retained the number one ranking by continuously enhancing the customer’s online banking experience, including industry leading performance in complementary account services and resources,” said Glenn LaCoste, President of Surviscor. RBC’s closest competitors in the rankings were Scotiabank, Bank of Montreal, TD Canada Trust, and Canadian Imperial Bank of Commerce (CIBC).

### Cohesion Will Ensure Take-Up

With each bank’s cashless payment options primarily benefiting its own customers only, it takes a whole industry pulling together for a new method to seem like the natural future. Beyond RBC’s Wallet, most major Canadian banks have launched some sort of mobile payment service in the past few years. CIBC offers a mobile payment app working on the Telus and Rogers networks, enabling customers to pay for low-cost goods by swiping the handset over an NFC payment reader. The Bank of Montreal provides a contactless payment tag, where customers can place a sticker containing the NFC technology on their handset. This is an interesting approach as it enables all the bank’s customers to get on the mobile payment system immediately, as they can put the sticker on their existing handset instead of needing to upgrade to a smartphone with NFC. Only 63% Canadians owned a smartphone in 2013, according to estimates from Visa. However by 2016, 80% are likely to own an NFC-enabled phone that can make contactless payments.

### The Future of Money

While Canadian banks are making good progress, critics argue the country still has a long way to go before it can claim to be successfully cashless. “In Canada today there are almost 10,000 bank branches, including credit unions. This branch structure costs well over C\$10bn to operate annually, or more than C\$300 per person in the country,” said John Armstrong, Managing Partner of financial services business and technology consultancy Capco.

“[Banks need to] work with other financial institutions and the regulatory authorities to upgrade Canada’s payments infrastructure. [...] While some progress has been made, the industry must adopt a more cooperative mindset to speed progress,” Armstrong wrote in national Canadian newspaper ‘The Globe and Mail’. In order to successfully push on towards cashlessness, banks need to focus on staying competitive through improved customer interaction, new product development, risk models or marketing strategy, argued Armstrong. While collaboration is taking place, Canadian banks could still do much more to take advantage of local innovation in the mobile payments arena: “These start-ups are often forced to look to the United States for funding and for charter customers. This is something that must change if [Canada] is to build an ecosystem of innovation around banking.”

In an acknowledgement that cash is not going away anytime soon, the Bank of Canada has over the past three years changed all its paper bills over to plastic. In addition to increasing the durability of each note, one of the main motivations for this move is curbing fraud. According to the Royal

Canadian Mounted Police, the number of counterfeit Canadian banknotes discovered in circulation in 2012, the first year after the introduction of plastic notes, was 92% lower than the peak in 2004. The cost of producing a plastic banknote is about 20 Canadian cents, compared to 11 cents for the old note. However, the plastic notes are expected to last at least 2.5 times longer.

Canada eliminated the one cent coin from circulation in 2012, in a move deemed so successful it has prompted calls for the five cent coin to be withdrawn as well. Canada is now saving an estimated C\$150 million a year by no longer producing the one cent coin, which cost more to produce than its face value. This is a problem faced by many countries with regards to their smallest coins; however, the elimination of small coins is more a consequence of value inflation than the cashlessness trend.

An interesting prospect as to what the future of cash may look like comes from the Royal Canadian Mint: a new digital currency called MintChip. MintChip was launched on a trial basis at the start of the year, described by the Mint as an exploration into potential future options to cash. Transactions using MintChip are anonymous and almost instantaneous, and should also be cheaper than standard bank transactions, according to the Mint. The difference from the similar BitCoin system is that the virtual currency is issued by the country’s central bank, which should hopefully avoid some of BitCoin’s issues with legitimacy, rapid value fluctuations, and lack of consumer protection.

MintChip is anchored in a cloud-based account, and users could make purchases with the virtual currency by downloading the MintChip app and tapping their phone to a payment terminal at checkout. “The Royal Canadian Mint has been a trusted and respected custodian of Canadian currency for more than 100 years,” said Ian Bennett, President and CEO of the Mint. “MintChip could be characterised as an evolution of physical money, with the added benefits of being electronic.” \*

■ Reporting by the Banking Insight Editorial Team.



**71%** OF CANADIANS  
ARE COMFORTABLE  
*with never having to  
handle cash to make a  
purchase.*

# Harmonising PAYMENTS THROUGH SEPA

THE **SINGLE EURO PAYMENTS AREA (SEPA)** WILL COME TO LIFE IN AUGUST 2014, HARMONISING PAYMENTS ACROSS EUROPE AND MAKING CROSS-BORDER PAYMENTS AND TRANSACTIONS ACROSS THE CONTINENT AS EASY AND LOCAL AS PAYING YOUR NEIGHBOUR.

I

magine a world where paying for something while abroad is just as easy as buying something at home - this is the promise of the Single Euro Payments Area (SEPA). This year sees the introduction of a unified payment system across Europe, a project that has taken 15 years to come to fruition.

Under SEPA, there will no longer be any difference between transactions made with someone in their home city, and with people in neighbouring European countries. This means payments and money transactions will be quicker, safer and more cost-effective, as payment structures have been harmonised across 34 countries.

According to the PwC report on 'Economic Impact of SEPA', SEPA could represent annual savings of as much as €21.9bn as stakeholders benefit from price convergence and process efficiency, assuming that all countries involved undertake not just the mandatory elements of SEPA, but also the voluntary practices. The European Central Bank (ECB) has been working on this since 1999, and the culmination is now a new set of payment instruments and common standards, plus a new legal basis for payments across the region.

## Harmonising Money Flow

"An efficient Single Market needs an efficient SEPA. The entire payments chain - consumers, banks, and businesses - will benefit from SEPA and its cheaper and faster payments. Cross-border payments are no longer exceptional events, which is why an efficient cross-border regime is needed," said Michel Barnier, EU Commissioner for the Internal Market.

SEPA covers the 28 countries in the European Union (EU), plus six more: Iceland, Liechtenstein, Monaco, Norway, San Marino, and Switzerland. Five hundred twenty three million people live in these countries, which are also home to about 9,300 institutions providing payment services. Under SEPA, all payments made in Euro are subject to the new regulations. For the first time, EU inhabitants will be able to pay a regular bill in one country using an account located in another country. The SEPA credit transfer ensures a single means of transferring funds regardless of whether it is a local or international transfer, with the same cost attached.

For banks, this meant adopting the International Bank Account Number (IBAN) identification standard: this includes a country code, a bank code and an account number. All payment cards have been migrated from magnetic strips to EMV chips, with the corresponding upgrade of payment terminals. Under SEPA, payment service providers must adhere to joint rules for cross-border and national credit transfers and direct debits, in a measure designed to ensure all the different payment systems are technically interoperable with one another.



SEPA covers the 28 countries in the European Union (EU), plus six more: Iceland, Liechtenstein, Monaco, Norway, San Marino and Switzerland.

### Deadline: 1 August

In January this year, 83.1% of credit transfers in the Eurozone were SEPA-compliant, according to the ECB; the same was true for 60.2% of direct debit transactions. 1 February 2014 was the original deadline for SEPA compliance for credit transfers and direct debits in the Eurozone. However, an additional six months has been granted to avoid disruption of payments from EU countries not yet ready.

“The stark risk of a business not complying with the SEPA standards is that its Euro payments or collections will not go through,” said Angus McFadyen, Technology and Payments Law Expert at law firm Pinsent Masons. “This is because they will not be sending the right messages in the right formats to their banks in order to allow their banks to effect those transactions.” The Royal Bank of Scotland’s report from January showed Estonia, Finland, Latvia and Slovakia had completed SEPA migrations, while the other countries are expected to complete the process at various dates between February and August.

EU members who use other currencies, such as the UK and Sweden, will need to ensure their Euro transactions comply with SEPA regulations by 31 October 2016. “Many corporates in the UK regard SEPA as a continental European project and believe they do not need to make efforts to comply. This is a risky approach for corporates that conduct Euro payments business in Eurozone countries,” said Jean Lassignardie, Global Head of Sales and Marketing at Capgemini Global Financial Services. In its 2013 ‘World Payments Report’, Capgemini found that financial groups across the SEPA region considered the changes as merely a regulatory burden, at least at first: “Right now, some corporates view SEPA as a compliance exercise that they need to meet, and less of an opportunity. However, its true benefits, such as centralisation of account receivables and straight-through reporting will be realised later.”

### Opportunities and Risks

The ability to trade across the whole Eurozone with an ease previously restricted only to the domestic market is one key benefit for businesses in the region. Furthermore, the 6,000 banks and 16.5 million companies across the Eurozone will also be able to automate much of the work related to payments and processing. This could potentially unlock as much as one million man years, according to PwC’s 2014 study ‘Economic Analysis of SEPA’.

“SEPA may unlock up to €227bn in liquidity and credit lines currently required for clearing transactions within the Eurozone. Furthermore, companies will be able to streamline their cash management infrastructures and close out up to nine million bank accounts,” said Didier Vandenhoute, Director of the Finance & Treasury Solutions Group at PwC Belgium. “Despite the loss in revenue due to price convergence, the banking sector should be able to benefit from increased process efficiency.”

While the latter point may prove to be the case over time, for now, SEPA has been slammed for eroding a traditionally lucrative income stream for banks; international money transfers and foreign card payments have traditionally been expensive for customers. Pre-SEPA, profits from payments have been substantial, equating to around a quarter of total banking revenues and 15% of banking profits, according to the Boston Consulting Group. In 2012, banks generated USD108bn in non-cash payments and transaction banking revenues in Western Europe.





### CONSEQUENCES

**While businesses in non-SEPA** regions which use banks in their own countries are unlikely to face the consequences of the new rules, the changes may actually make it more beneficial for them to establish a relationship with an European bank if they do a lot of business there.

### Beyond Europe

The SEPA initiative also stands to impact countries outside the Eurozone. Switzerland and San Marino have opted to join SEPA in order to benefit from smoother payment flows when trading with the Eurozone. Beyond becoming a full member, any country could informally adopt parts of SEPA according to its needs; the ECB has based the SEPA payment instruments on open, global standards, and the rulebooks for SEPA credit transfers and SEPA direct debits are in the public domain.

“To address the requirements of a modern economy, many emerging countries are rethinking the set-up of their retail payment infrastructures,” said Wiebe Ruttenberg, Head of the Market Integration Division at the ECB. “What is interesting is the potential the SEPA experience entails for financial inclusion. Affordable, efficient and safe retail payments are conducive to a developed and inclusive economic and social environment. Such payments represent the basis on which to build innovative solutions; standardisation and a level playing field are also conditions for a more competitive market.” Beyond the national advantages, Ruttenberg pointed to SEPA’s potential of representing “a benchmark of financial integration for regions which would like to make the next steps on the way to an economic or monetary union.”

Businesses located in non-SEPA countries will have to comply with the new regulations if they use a European bank to make transactions there. “Whether or not there are costs associated to this in the short term, it is probably more important to emphasise the benefits SEPA will bring in terms of harmonisation and standardisation: once a payment has been converted into SEPA standards, it has the potential to reach 34 SEPA countries without additional complexities,” said Ruttenberg, who is also the coordinator of SEPA efforts between the ECB and the 18 central banks across the Eurozone.

While businesses in non-SEPA regions which use banks in their own countries are unlikely to face the consequences of the new rules, the changes may actually make it more beneficial for them to establish a relationship with an European bank if they do a lot of business there. Jeroen Kok, Executive Director of J.P. Morgan Treasury Services in Singapore, pointed out that international companies would be missing an opportunity if they dismiss SEPA as irrelevant.

“SEPA offers a unique and very real opportunity for treasurers to achieve far greater benefits by rationalising payments practices, enhancing processes and reducing the cost of payments and banking fees. One major reason corporations are able to achieve these benefits is that SEPA will enable them to make all their Euro payments out of one account, significantly reducing the number of bank accounts and simplifying the liquidity structures.”

Just as SEPA will benefit European companies and individuals who currently have accounts in multiple countries, international companies will be able to streamline paperwork and costs by having just one bank account to send and receive money in Europe. “Using just one account will also immediately concentrate funding and liquidity, thereby reducing the need for physical and or notional forms of cash pooling. [This] simplifies the process of managing liquidity and enables better operational risk management,” said Kok.

SEPA stands to simplify Europe as a potential market for Asian companies who want to expand into this region, argued Mahesh Kini, Asia Pacific Head of Cash Management for Corporates, Global Transaction Banking at Deutsche Bank. “Asia-based companies operating in several European countries have always had to establish a two-tier operating structure, with both in-country bank accounts to facilitate local payments and collections in each country, and an overlay account structure in one of the financial hubs in Europe to consolidate Euro liquidity.” This meant companies needed several

bank accounts, which then all had to be audited every year, adding cost and time to the process. This issue goes away with SEPA.

Having said this, Kini still believes Asian companies have work to do before they can fully take advantage of the SEPA opportunity: "There are still many Asian companies that need to get up to speed with SEPA. Given the adoption rate thus far among European corporates there is clearly still a lot to do there, and being based further away, Asian companies are likely to have an even greater need to become more familiar with the requirements and benefits of SEPA."

### SEPA - An Inspiration?

If SEPA becomes a success story, the scheme has the potential to inspire other regions to initiate their own joint payment infrastructure. Globally, the International Payments Framework Association (IPFA) is already such an initiative. The IPFA works to facilitate cross-border payments at global level via common technical standards, business practices and interoperability. Regionally, examples of economic integration include the African Economic Community, and the ASEAN Economic Community (AEC).

"Of course, the SEPA project itself is open to inspiration from outside," said ECB's Ruttenberg. "We are paying attention to what happens in other regions of the world, also considering that technology is blurring geographical boundaries and any regional solution might be exposed to global influences." Asked whether the AEC could draw inspiration from SEPA, Ruttenberg emphasised this would very much depend on the specifics of the Asian market, but suggested it may be advisable to adopt international standards to lay the foundations for an integrated environment. Doing this would avoid having to remedy fragmentation at a later point. "SEPA adopts open, international standards that are already used in other regions of the world. For example, IPFA aims to spread the use of harmonised standards for international

credit transfers such as the ISO 20022, which is already the standard for SEPA payments. Projects for faster payments in Singapore are reported to make use of ISO 20022, just like SEPA payments. [The use of international standards] fosters business practices that can in principle be reproduced elsewhere," said Ruttenberg.

In any case, the AEC and other regional initiatives will be studying the implementation of SEPA this year, and its progress and obstacles in the years to come. Public authorities acting as catalyst for change need to encourage not only competition in the market, but also a necessary degree of cooperation among competitors to agree on common standards and achieve interoperability,

said Ruttenberg. Equally important is "striking the right balance between self-regulation and regulation, since market players alone might lack incentives to attain socially optimal results, at least in a reasonable time frame."

Another lesson from the development of SEPA is "involving stakeholders from both the supply and the demand side of the market at governance level. Involving users is crucial since retail payments have become a commodity, and are essential for participation in the economic and social file." Lastly, Ruttenberg recommended fostering cooperation and dialogue between many stakeholders from public authorities and the private sector when implementing such a wide-ranging system.

## Looking to 2016

While August's SEPA deadline is the end of a journey that has taken 15 years to complete, there is still work left before Europe can fully and truly become a single payment area. "The most obvious outstanding issues will be the continued use of local niche products and non-SEPA compliant products. [...] Without further standardisation, banks will compete locally in only half-open markets," said PwC's Vandenhoute. "Even though the end-date is set for niche products, companies will need local bank accounts in their cash management infrastructure up until 2016."

**While August's SEPA deadline is the end of a journey that has taken 15 years to complete, there is still work left before Europe can fully and truly become a single payment area.**

Another factor preventing the full fruition of SEPA is the requirement of several European countries that residents and companies maintain local accounts for national tax and social security payments. "Local governments might decide they need to change their processes to fully benefit from increasing competition in the banking sector," said Vandenhoute.

While many of the SEPA regulations are mandatory as part of EU law, there are numerous potential benefits to the system which can only be accessed if the member countries are willing to go the extra mile. "Defining and implementing common technical standards is not in itself sufficient for delivering on the promises made," concluded Vandenhoute. "The full €21.9bn of [potential] savings depends on a harmonised strategy for non-mandatory specifications and resolving conflicts of interest before markets can be integrated and a level playing field is created across the SEPA zone." \*

■ Reporting by the *Banking Insight* Editorial Team.

# Bitcoins:

*aye*

OR

*nay?*

**WILL A SPATE OF BAD NEWS FOR BITCOINS** RESULT IN AN EVENTUAL BLANKET BAN ON THIS GLOBAL VIRTUAL CURRENCY? OR WILL BITCOIN'S INNOVATIVE DISRUPTION CHANGE THE FACE OF FINANCIAL SERVICES FOREVER?

■ PREETHA NADARAJAH



**I**N RECENT MONTHS, there has been no shortage of bad news for bitcoins: the downfall of the revamped second Silk Road, a popular marketplace for drugs and other contraband; the arrest of a high-profile member of the Bitcoin Foundation for money laundering; and the ban of bitcoin in Russia and Vietnam. Adding insult to injury, politicians are putting pressure for a broader ban on bitcoin following February 2014's publicity crisis when the world's first bitcoin exchange MtGox, filed for bankruptcy in Japan.

As a result of these recent issues, there have been many cautionary notes against the use of bitcoins or even outright barring of bitcoin trading by central banks worldwide. More likely than not, the status of bitcoins will continue to be very fluid. Can bitcoins pose a challenge to 'fiat' currencies? Or will it end up in the graveyard of other virtual currencies?



## Looking Back at Virtual Currencies

Virtual currencies have risen and fallen for decades with the bitcoin being the virtual cryptocurrency *du jour*. History is littered with virtual currency wreckages ranging from the prominent Second Life's Linden Dollars (L\$) launched in 2003 and used in Second Life's multiplayer online role-playing game, through to the e-gold, a digital currency then managed by E-Gold Ltd, a company registered in the lightly regulated Caribbean haven of Nevis.

One of the key issues that ultimately caused the downfall of the Linden Dollars was the holes in regulation. There was only one authority and regulator for L\$, called the Linden Lab, which could control every aspect of the virtual community but lacked proper legal basis and oversight. E-Gold's mixture of anonymity and irreversible transactions made the service a haven for crime syndicates looking to convert dirty dollars into clean cash. In 2008, the founder of E-Gold pled guilty to money laundering and operating an unlicensed money transfer business and the US government froze all account holder funds.

Despite the bumpy road that virtual currencies have travelled for decades, the demise of bitcoin might not be a foregone conclusion. Even mainstream institutions have put bitcoin on their radar. The Bank of America is the first major Wall Street bank to issue an opinion on the bitcoin, which has grown in prominence since its debut in 2009. Instead of predicting the inevitable doom of bitcoin, in a December 2013 research report, analysts at Bank of America's wealth management division, Merrill Lynch, estimated bitcoin's maximum market capitalisation to be at USD15bn and placed a maximum fair value of USD1,300 per bitcoin.

## What is bitcoin?

Bitcoin is a digital currency designed by Satoshi Nakamoto, a pseudonym, in early 2009. Bitcoin allows users to send payments within a decentralised, peer-to-peer network made up of many 'miners', and is unique in that it does not require a central clearing house or financial institution clearing transactions, unlike some of its virtual currency predecessors, e.g. L\$ in the Second Life. Users must have an internet connection and bitcoin software on their computer or mobile device to make payments to another public account or address.

A public history of all transactions is continuously updated and verified by independent and decentralised 'miners', which are specialised computers that gather batches of new transactions into blocks and attach these blocks to the end of the 'Blockchain'.

Given the use of public-key cryptography in bitcoin, some level of anonymity is possible within this publicly available ledger, although not complete anonymity, in contrast to yet another virtual currency predecessor, the e-gold. A block of transactions has to be agreed among the majority of the miners in the network before it can be added to the blockchain. Any rogue computer is just ignored by the rest, thereby assuring that no single miner could rule the network. The inherent decentralised and geographically distributed nature of this network means that there is no one central point of authority or country to be held accountable.

Bitcoin miners are incentivised when they earn transaction fees in terms of bitcoins paid by users for faster transaction processing. A bitcoin miner's profit comes from managing the overhead costs of the specialised hardware infrastructure

versus the revenue from the market value of bitcoins received. New bitcoins are only created and introduced into the system when the increasingly complex algorithm is solved demanding increasing computing resources. This design aims to ensure that the supply of bitcoins could not then be altered by a central authority or participant wanting to print extra money. As such, the intent of this system is to avoid inflation as well as the business cycles originating from extensive money creation.

Bitcoins can be bought and sold at bitcoin exchanges for the US dollar, the Chinese yuan renminbi and other 'fiat' currencies. There are a handful of popular exchanges that manage most of the worldwide exchange of bitcoins for 'fiat' currency and vice versa, as indicated in Table 1.

### How Does Bitcoins Stack Up Against 'Fiat' Currency?

In a provocatively titled December 2013 research report 'Bitcoin to Replace AUD?', Emma Lawson, from the National Australia Bank (NAB), one of Australia's big four banking groups, said that: "Bitcoins can indeed be currency, as could anything labelled as such. As long as you believe it is."

"Bitcoin comes about as a response to quantitative easing and concern regarding central banks' printing money. But what it cannot replicate is the revenue generating abilities of central banks and the governments that control them, or their inflation fighting credentials. Neither does it have the centuries of history that gold is backed by," she concluded.

**Based on the textbook definition, money is traditionally associated with three different functions:**

- **MEDIUM OF EXCHANGE:** money is used as an intermediary in trade to avoid the inconveniences of a barter system.
- **UNIT OF ACCOUNT:** money acts as a standard numerical unit for the measurement of value and costs of goods, services, assets and liabilities.
- **STORE OF VALUE:** money can be saved and retrieved in the future.

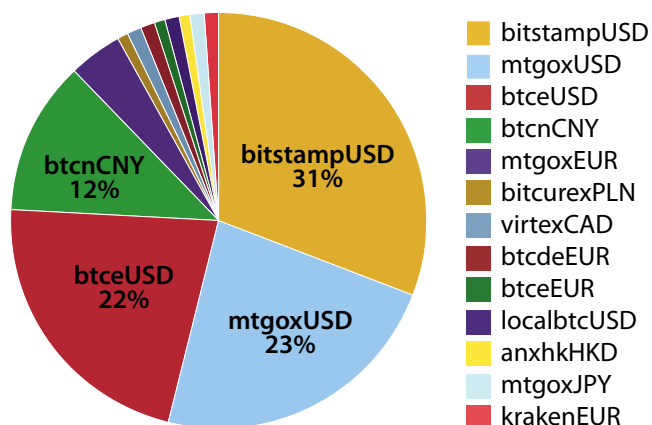
Bitcoin is attractive as a medium of exchange, offering reduced transaction costs by eliminating the need for a central clearing house or financial institution to act as a third party to financial transactions. Also, by virtue of the bitcoin network being global, cross-border payments or remittances are quicker in contrast to the traditional methods of bank transfers or via payment operators such as MoneyGram or Western Union.

In estimating the fair value of the bitcoin, the Merrill Lynch team concluded that the market capitalisation of the bitcoin would be approximately USD5bn for B2C (business-

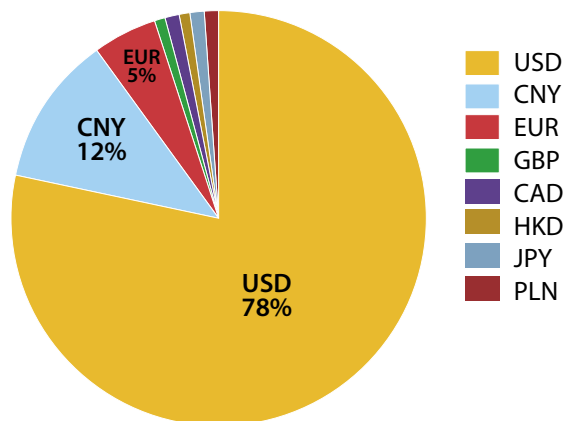
**TABLE 1:**

Volume distribution by bitcoin exchange and currency traded as of 15 February 2014. Source: <http://bitcoincharts.com/charts/volumepie/>

### Exchange volume distribution by market



### by currency



to-consumer) e-commerce transactions and another USD4.5bn for remittances. This assumes that bitcoin could become one of the top three players in the money transfer industry, taking about 20% market share from the existing players and assuming negligible contribution of bitcoin for B2B transactions. Based on these staggering estimates, and regardless of the future of bitcoin as a 'fiat' currency, the mere existence of this bitcoin technology could clearly be the trigger for a structural change in the financial services industry, specifically in as far as remittances go.

## Bitcoin Exchange Security Concerns

Like other forms of currency, bitcoin does pose security concerns. It is possible for hackers to access bitcoin wallets and drain them electronically, but it seems no easier to carry out on a large scale than theft of money. Similarly, robbing the electronic wallet is just as possible as it is for the physical wallet which holds 'fiat' currency.

However, the suspect quality of security on bitcoin exchanges, where consumers exchange dollars for bitcoins (and vice versa) is a stumbling block. The recent MtGox bankruptcy filing attests to this.

MtGox, the bitcoin exchange that enjoyed first mover advantage and once ranked as the world's largest bitcoin exchange, has been plagued with problems for a long time and can hardly be described as reliable. In mid-2011, a hacker into MtGox issued sell orders for hundreds of thousands of fake bitcoins, briefly driving the price down from USD17.50

to USD0.01. In May 2013, US authorities seized around USD5 million on the grounds that MtGox was operating as a money transmitter without being properly registered. In June 2013, the US dollar withdrawals were suspended and reinstated a month later. What seemed to be the final nail in the coffin was the recent fiasco in February 2014, when MtGox filed for bankruptcy protection in Japan as USD500 million worth of bitcoins, or around 850,000 bitcoins, had gone missing

after weeks of sustained DDoS (distributed denial-of-service) attacks and what the bitcoin developers termed as 'transaction malleability' problems. Given that the latter is a well-known loophole in the bitcoin system since 2011, which has workarounds available, the management of the exchange was blamed and there were requests that such exchanges be regulated. Other smaller exchanges have also been attacked and have lost smaller numbers of bitcoins. This is where 'fiat' currency has the advantage of deposit or investment protection, which bitcoin lacks. Since there is limited legal protection for bitcoin, investors and users need to be mindful that they are exposed to investment risks as well as credit risks.

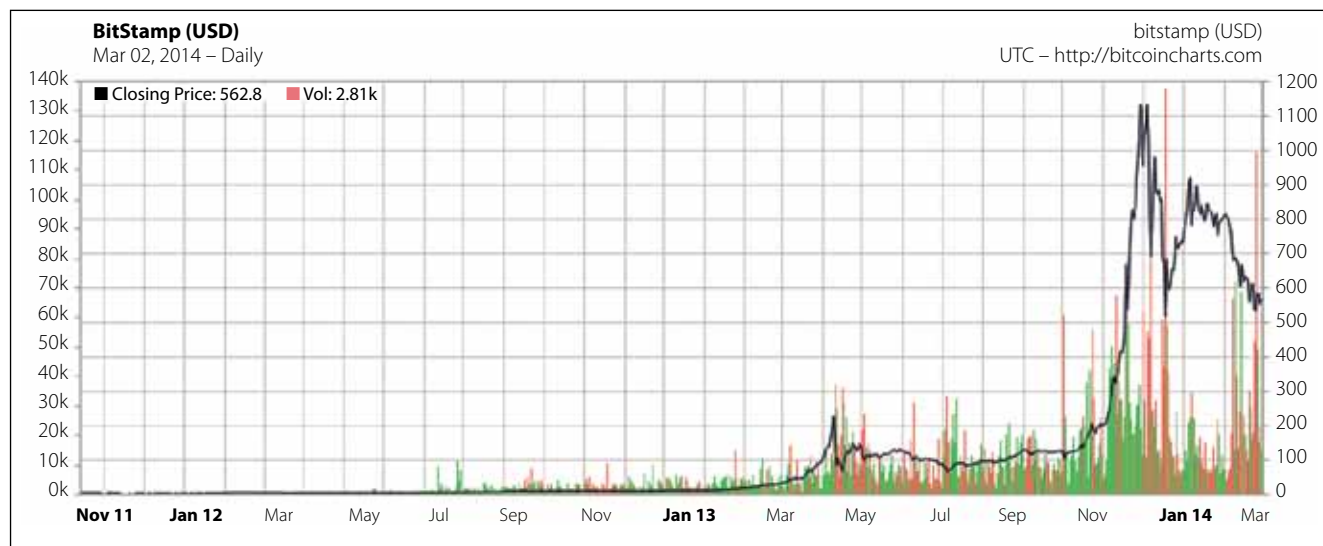


## Limited Bitcoin Supply Akin to Former Gold Standards

By design of an open-source community project to which many software developers continue to contribute, the maximum number of bitcoins in circulation by 2140 is expected to be 21 million bitcoins or 2,100 trillion satoshi, the smallest unit of bitcoin, with just below 58% of this currently in circulation. Those who criticise the current fractional-reserve banking system – whereby banks can extend their credit supply above their actual reserves and depositors can simultaneously withdraw their funds in their current accounts at any time – are proponents of this design which is inspired by the former gold standards.

## Store of Value Impacted by Bitcoin's High Volatility

The value of a bitcoin is determined based on market supply and demand similar to the foreign exchange market. The bitcoin started in 2013 at a low of about USD10 to a high of about USD1,100 in December 2013 before closing the year at about USD800. In late February 2014, the price of bitcoin had declined to the USD500-600 range.

**TABLE 2:** Daily closing price on the BitStamp bitcoin exchange, one of the larger exchanges globally.

Given the highly anonymous nature of bitcoin and the way the distributed and decentralised bitcoin network functions, apart from geeks, speculators and libertarians, the early adopters of bitcoins have been those involved in illegal activities such as drug dealing and money laundering. Bitcoins are also perfect for getting around tight capital controls imposed by the state, which prevent the rich from moving too much money overseas, which may explain why one of the largest bitcoin exchanges is based in China and why the dominant currency traded is the US dollar, followed by the Chinese yuan renminbi and then euro.

Definitely, its volatility and its use in speculation affects its acceptance, credibility and viability as a medium of exchange.

As a store of value, bitcoins have no intrinsic value like gold or silver do; they are mere bits stored in a computer and unlike precious metals, are not backed by reputation and a long history of usage. Furthermore, given that bitcoins do not pay any interest and no investment instruments currently exist that are denominated in bitcoin, Merrill Lynch reportedly estimated the maximum market capitalisation of bitcoin as a store of value at about USD5bn, which is below the USD8bn value of total US silver eagles minted (since 1986) at the time of writing.

### Business Opportunities in Bitcoins

Digital technology companies are backing the supporting systems for virtual currencies. This implies that whilst the future for bitcoin remains opaque, it must be acknowledged that the demand for innovative payment systems is here to stay. For example, Asia's richest man, self-made billionaire Li Ka-shing, has invested an undisclosed amount into BitPay,

a start-up with ambitions to become the PayPal of the bitcoin world via his Hong Kong-based company, Horizons Ventures which is focused on disruptive technology. Prior to this, Founder's Fund, a venture capital (VC) firm started by what is commonly called the PayPal Mafia (comprising ex-employees and founders of the payments innovator) has also invested USD2 million into BitPay. BitPay reportedly handles transactions for around 14,000 companies in over 200 countries.

Meanwhile, a second *eBay* patent titled 'System and Method for Managing Transactions in a Digital Marketplace' has surfaced on the US Patent and Trademark Office database. The patent highlights *eBay's* interest in digital currencies and digital currency processing systems, naming bitcoin specifically along with other forms of virtual currency. The patent was filed in 2011, indicating the global marketplace giant's early interest in incorporating virtual currencies as part of its online payment systems.

Microsoft too has shown interest in this space. Even as far back as 2011, in the context of a survey on innovation in payment systems carried out by the Reserve Bank of Australia (RBA), Microsoft had asked the Australian central bank to consider adjustments to the domestic payments market to help consumers conduct transactions in virtual currencies.

In addition to the digital technology companies creating opportunities with bitcoins or virtual currencies in general, there has also been movement in the ancillary financial services industry. Hedge funds such as Exante and Fortress with USD45 million and USD150 million in assets under management have been set up in the last couple of years in support of the bitcoin industry and catering for the wealthy.



The Winklevoss twins, famous for their legal battle with Facebook founder Mark Zuckerberg, are also working with the U.S. Securities and Exchange Commission (SEC) towards the creation of a bitcoin exchange traded fund (ETF) towards the end of 2014. The Winkdex index will use as its benchmark the data from seven bitcoin exchanges and weigh the prices based on the volume of trading on each exchange. If this materialises, it would then in turn create an opportunity for the stock exchange on which the ETF would then be traded.

The emergence of this virtual currency has also created new growth opportunities for existing businesses that make up the components of the supply chain of the bitcoin network. A January 2014 Wedbush Securities

equity research report estimated that more than USD200 million has been spent on bitcoin network mining and most of this on the significant technology providers, the chip fabricators Taiwan Semiconductor Manufacturing and Advanced Micro Devices (AMD). Bitcoin ATMs by Lamassu and Robocoin are also starting to be rolled out in some countries.

On a smaller scale and closer to home, *bitcoinmalaysia.com* leases hashing power to miners allowing them to save on the capital expenditure of purchasing and managing specialised ASIC (application-specific integrated circuit) servers. *BTC-asia.com* provides bitcoin escrow services for buyers and sellers, charging a flat-rate fee per transaction.

## Force of Disruption

*Napster* created an upheaval in the music industry by creating a platform where users around the world could exchange music in an mp3 format online, combining the innovations of digital music and the Internet. Unfortunately, it was eventually forced to shut down by the music industry due to copyright infringements. Then came the *iTunes* business model, allowing technology to be maximised without ignoring intellectual property and achieving a similar result for the end-users, much to the chagrin of brick-and-mortar retailers such as HMV, Tower Records and Virgin Megastores, which sold the physical and higher-cost music CDs. Since then, the number of these music stores have been dwindling although we may fondly remember the heydays when these stores ruled the high streets.



Could bitcoin be the disruptive innovation to the financial services industry today, as *Napster* was to the music industry? Or should the parallels be drawn for the bitcoin against *iTunes* instead? Time will tell whether bitcoin can overcome the cornucopia of security threats, adoption rate and volatility. Stay tuned. This space is changing and changing rapidly, at that. \*

# Policing Bitcoin

Regulatory stances on independent virtual currencies could determine bitcoin's long-term sustainability. And if bitcoin takes off, pioneering governments that move early to lay down fundamental regulations for bitcoin could seize unfolding opportunities in the virtual currencies ecosystem.

■ PREETHA NADARAJAH



# A

t this stage, it is a little too early to predict the eventual changes that the bitcoin technology will bring about. Bitcoin could be the next big

revolution after the Internet, or it could become another virtual currency wreckage.

Regulatory policies, positive or negative, are a key factor that could determine bitcoin's prospects. Currently, it is clear that governments remain divided on this controversial cryptocurrency. However, pioneering governments that move early to lay down fundamental regulations for bitcoin could seize unfolding opportunities in the virtual currencies ecosystems.

## Differing Regulatory Stances

In November 2013, bitcoin purportedly got a mainstream nod when Federal Reserve Chairman Ben Bernanke said that "there are also areas in which they (bitcoins) may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system."

China took the opposite tack. About a month after Bernanke's remarks, China's central bank, the People's Bank of China (PBOC) not only cautioned the public on bitcoin, but moved to bar all local third party payment providers from offering clearing services for digital currency exchanges, such as bitcoin. This effectively removed the means for the Chinese to make new purchases of bitcoins on these exchanges. However, individuals in China are still legally allowed to buy and sell bitcoins on the Internet at their own risk.

In December 2013, the Central Bank of Korea (BOK) and other South Korean authorities concluded after a week of debate that the bitcoin currency had no 'intrinsic value' due to its lack of stability and raised concerns over the economic feasibility of this virtual currency. Given the limited security measures in light of increasing malware attacks on bitcoin miners and DDoS (distributed denial-of-service) attacks on bitcoin exchanges, BOK was doubtful on the potential of bitcoin as a future means of exchange.

ASEAN central banks too are proceeding with caution. In early January 2014, Bank Negara Malaysia issued a statement cautioning the public on the risks of using bitcoin. The

bank stated that it is not legal tender in Malaysia and is not regulated by Bank Negara Malaysia.

Bank Indonesia issued a similar message for Indonesians in early February 2014, but there will be limited impact given users are in the minority. Despite being the fourth most populous nation worldwide, it is estimated that Indonesia currently accounts for only around 1% of total world bitcoin usage.

Bangkok had a change of heart on bitcoin. In July 2013, following a bid to the Central Bank of Thailand to set up and operate a bitcoin exchange in Thailand, Bitcoin Co. Ltd was advised that “due to lack of existing applicable laws, capital controls and the fact that bitcoin straddles multiple financial facets, that bitcoin activities are illegal in Thailand.” After further consideration, in January 2014, in a letter to Bitcoin Co. Ltd., the Central Bank of Thailand stated that “Bitcoin exchange operations do not fall under the scope of the Ministry of Finance regulation, unless foreign currencies are also offered for exchange.” The bitcoin exchange has since commenced bitcoin trading within Thailand using Thai baht as of February 2014.

## First Movers in Bitcoin Regulation

Perhaps reflecting Singapore’s more developed and sophisticated market, the Monetary Authority of Singapore (MAS) announced in December 2013 that it will not intervene in a business decision to accept bitcoins in exchange for goods and services. Bitcoin transactions are “a commercial decision in which MAS does not intervene.”

Taxation authorities are also getting in on the bitcoin game. As of 2014, the Singapore Inland Revenue Authority laid out taxation rules governing bitcoin services located in Singapore. Profits from businesses that buy or sell goods or services using virtual currencies, bitcoin mining and trading of virtual currencies need to be taxed as per normal Singapore income tax rules.

However, businesses that reap capital gains from long-term investments of virtual currencies will be exempt from capital gains tax since such gains are not subject to tax in Singapore.

In the case of goods and services tax (GST), the sale or exchange of bitcoins in return for cash or in kind is considered a “taxable supply of services.” Thus, when bitcoins are accepted for goods or services, if both parties are GST-registered, GST will be imposed. Virtual goods and services, such as apps, will not be taxed. Middlemen involved in bitcoin trading will also find themselves subject to GST on their commission fees and on the sale of bitcoins.

The fact that Singapore, one of the world’s top financial hubs, is now laying the regulatory foundations for virtual currencies, gives credence to bitcoin. For Singapore, it is a pragmatic decision. It indicates that Singapore desires first mover advantage in obtaining the venture capital investments that are going into the virtual currency ecosystems.

Over in Europe, Luxembourg too is laying tracks in the arena of virtual currencies. In mid-February 2014, interested businesses aiming to facilitate digital currency-related commerce in Luxembourg were invited to apply to CSSF (Commission de Surveillance du Secteur Financier), the government body responsible for financial regulation in Luxembourg, to seek approval for activities related to virtual currencies. Examples included the issuing of means of payments in the form of virtual or other currencies; the provision of payment services using virtual or other currencies; and the creation of a market (platform) to trade virtual or other currencies.

## Competing for Global Capital

CoinDesk’s first ever ‘State of Bitcoin 2014’ report released in February 2014, states that USD97.5 million venture capital (VC) investment funds were



invested in 30 bitcoin related start-ups in 2012-2013.

Sixty per cent of these start-ups are based in North America, 30% in Asia and 10% in Europe. In Asia, three start-ups are based in China and there are two each in South Korea, Singapore and Australia. The Asian start-ups received 14% of VC funding, with China taking up 8% of this investment, Singapore 4%, South Korea and Australia taking 1% each, while the US start-ups received about 70% of the value of the VC investments.

In comparison, VC investment in the Internet in 1995 was about USD508 million. Total VC investment in the

Internet was USD7.2bn from 1995-2013, an increase of more than 14 times over the course of eight years.

Those likening bitcoin’s revolution to that of the Internet when the latter was first introduced, then go on to infer that the 2012-2013 VC investment of

USD97.5 million in bitcoin start-

ups is likely to increase exponentially from current levels. At merely half of the proportion of spend on the Internet boom, or seven times that of the current investment levels, VC investments in bitcoin start-ups could reach USD700 million over the next eight years or so.

CoinDesk is a global publication providing news, prices and information on bitcoin and other digital currencies. Caveats to the numbers presented are that due to limited data availability, only publicly reported VC investments could be tracked and that data for the Internet was only available as of 1995 and so it does not cover the Internet infancy years from 1993 leading up to 1995. \*

■ Preetha Nadarajah is a freelance writer based in Kuala Lumpur.

*Bitcoin could be the next big revolution after the Internet, or it could become another virtual currency wreckage.*

# *Crowdfunding* **takes off**

STARTING OUT AS A WAY TO THROW SOME CASH AT STRUGGLING MUSICIANS, CROWDFUNDING IS EMERGING AS A VIABLE FINANCING AND INVESTING ALTERNATIVE FOR CREDIT-HUNGRY BUSINESSES SEEKING LOANS AND EQUITY. WHILE THE GLOBAL VOLUME OF CROWDFUNDING REMAINS SMALL, ITS RAPID GROWTH AND ACCESSIBILITY COULD OFFER LESSONS IN LENDING FOR TRADITIONAL FINANCIAL INSTITUTIONS.

■ JESSICA FURSETH



**CROWD  
FUNDING**



hey say necessity is the mother of invention - this would certainly explain why a brand new way for companies to access capital has emerged from a recession.

Crowdfunding is the model that sprang up to fill the void when banks were reluctant to provide development cash for small companies during the economic downturn. For UK businesses, there is now a £84bn to £191bn gap in funding over the next four years, according to a study by a UK government-appointed committee. But if banks do not want to step up to lend, there are others who might.

Of course, business equity was not what crowdfunding originally set out to do. Born in the creative industries, the first crowdfunding platforms were Kickstarter and Indiegogo, where musicians and artists could reach out to fans for cash for their next projects. Sometimes contributors would be rewarded with a copy of the product, but often the payback came in knowing that they had helped sustain the creative process and supported an artist or project which they believed in.

This was the inspiration for equity crowdfunding or peer-to-peer lending, which is gaining traction as a genuine alternative for businesses trying to access funding. For investors, the structuring of crowdfunding platforms is also improving – instead of just donations, investors can offer loans with interest or investments which provide a return on equity if and when the company in question performs well.



## An Increasingly Global Market

Crowdfunding campaigns across the globe raised nearly USD2.7bn in 2012 through all crowdfunding business models and platform types, according to the World Bank. USD1.6bn of this was raised in North America, financing over a million projects including start-ups, scientific research, community projects and games. USD945 million was raised in Europe, with the remaining USD110 million in the rest of the world. Across all regions, crowdfunding expanded at a 63% compound annual growth rate (CAGR) from 2009 through 2012.

“While the recent global recession has played a part, advancements in technology are also a significant driver of the recent growth of this type of model,” said Yannis Pierrakis, Head of Investments Research at the National Endowment for Science, Technology and the Arts (Nesta), the UK innovation foundation. “The proliferation of internet use and growth in social media has enabled those seeking finance to reach more people with greater ease and at far less cost. The ability to securely transfer money online allows those seeking to back a project or business to safely contribute funds. And the increase in the quality and volume of data available on individuals and businesses finances allow for the creation of accurate credit scores, which allow lenders to set suitable interest rates on the finance they offer.”

It is still early days for crowdfunding, and Nesta’s 2013 report, ‘Banking on Each Other’, concluded it remains to be seen whether this kind of business lending will be sustainable over time. Still, studies by peer-to-peer lender Funding Circle have suggested companies are increasingly open to considering crowdfunding as a funding option, as long as the platforms provide attractive facilities. While 60% of businesses who approached Funding Circle had tried banks first, 77% said they would go straight to the crowdfunder next time. Speedy processing, good interest rates, clarity of terms, and an easy-to-use platform was cited among reasons for preferring Funding Circle over banks.





### Crowdfunding Goes Pro

Last year, UK fund management veteran Nicola Horlick raised £150,000 for her new film finance company, Glenthams Capital, in just 22 hours through equity crowdfunding site Seedrs. About 135 investors chipped in to meet the funding target, which represents 10% of the new company. All UK-residing adults are eligible to invest via Seedrs, provided they pass a quiz showing they understand the risks of early-stage investing. Contributions can start as low as £10. Seedrs carries out due diligence on all the companies on the platform, and takes 7.5% of the funds raised, as well as 7.5% of any profit made by an investor through an exit or dividend.

“Having been a fund manager for the past 30 years, I know what a great opportunity it can be to invest in a fund management company. In the old days, there was no way that I could have opened an opportunity like this to the crowds, but Seedrs provides me with the perfect opportunity to do so,” said Horlick, who is now planning her own crowdfunding platform: Money&Co. “Our platform will let people lend to businesses at a rate agreed by both parties. It is a smarter way for businesses to get the capital they need and for people to get a better return on their cash,” said Horlick. “At the moment, banks are not doing enough for credit-worthy businesses. Money&Co will bring together good businesses that need to borrow to expand, with people who want to save at a more attractive rate than the banks offer.”

Money&Co will join Seedrs and Crowdcube in their mission to fund UK companies. SyndicateRooms and InvestingZone are among newer entrants to the market. Specialist platforms include MoolaHoop, focusing on women entrepreneurs, and Trillion Fund, targeting renewable energy projects. In the US, Crowdfunder, CircleUp and RocketHub have joined Kickstarter and Indiegogo in a market that now has over 300 platforms. These include Somolend which specialises in loans for small businesses, and Appbackr which focuses on fundraising for new apps. AngelList is among established names in Silicon Valley, connecting professional investors with start-ups.

### Regulating a Young Industry

The US crowdfunding market got a boost last year when the Securities and Exchange Commission (SEC) changed the rules to allow companies to sell stock via these platforms. Previously, shares could only be sold if they were registered, a process that can be costly for small companies. The SEC's new rules, politically prompted as a means for job creation, have been well received in the industry as likely to encourage growth. “The way the world has worked in early stage investing has been fairly stable over the last 20 years. The argument is that it is hard to manage investors, time-consuming to communicate with them, and challenging to gather their votes,” said Sherwood Neiss, Co-Founder and Principal of Crowdfund Capital Advisors. “The data demonstrates, however, that while some investors may be saying negative things about crowdfunding, others are using this new tool for deal flow.” Data from Crowdfund Capital Advisors suggests 28% of companies had closed an angel investor or venture capital round within three months of crowdfunding, while an additional 43% were in discussions with institutional investors.

Having said that, this remains a crucial time for the crowdfunding industry to get its foundations right; the theoretical potential for scandal is there if practices are careless or investor education poor. Wrote Neiss in ‘VentureBeat’: “The [SEC] rules need to maintain the ability for investors to sue for fraud, while reducing lawsuits against companies that just fail. Even though the legislation mandates that investors complete an education series on crowdfunding, investors should also be required to sign a document acknowledging they could lose all their money, (and) that they are responsible for reviewing the investment materials prior to investing.”

Also keen to see a solid foundation built for this budding industry, the UK's Financial Conduct Authority (FCA) announced a new set of rules for crowdfunding in March. This included a requirement that non-professional investors do not invest more than 10% of their savings per year, a move criticised as excessively strict by the industry. The FCA, however, pointed to the ‘significant risk of failure’ on the part of the companies seeking funding as a motivator for protecting investors from getting in too deep. “We are trying to strike a balance between on one hand making sure consumers are properly informed and have real clarity about the investments they are getting into, and on the other hand, making sure this [...] source of funding is open to businesses and individuals,” Chris Woolard, Director of Policy, Risk and Research at the FCA, told the BBC.

## Enter Asia

While crowdfunding has yet to make the same waves in Asian markets, this may only be a matter of time. Singapore, Korea, Brunei and Malaysia have started showing interest in rewards-based portals, as several platforms were launched in Asia in the last couple of years. Pozible is an Australian platform that expanded into Singapore and Malaysia earlier this year. “We are working to build up our user base in Asia, and these efforts are already starting to show developments, with an increase in Asian projects and Asian web traffic,” Pozible Co-Founder and Director Rick Chen told *TechCrunch*. Focusing on funding creative projects, the company wants to differentiate itself by becoming a specialist in the region.

Swedish site FundedByMe entered the Singapore market last year, offering the option for local businesses to raise money in exchange for equity. “We see Singapore as the gateway to Asia. We will be reaching a massive new market of potential crowd investors who are eager to help us build on the cross-border investment motion that has made FundedByMe a popular choice for European investors,” said Daniel Daboczy, CEO and Co-Founder of FundedByMe. “Early feedback tells us that Asian investors are keeping a keen eye on the European start-up scene, and vice versa.”

Earlier in 2013, Singapore’s own Crowdonomic stepped up to provide a professional crowdfunding service for businesses. However, Leo Shimada, Founder and Managing Director of Crowdonomic, told *Fortune* there are several reasons why the region has yet to fully embrace this funding model. The absence of a high-profile frontrunner like Kickstarter is one, as this means the concept is still alien to much of the general public. Local culture is another reason, said Shimada: “Wherever you are in the world, no one wants to be a loser, but especially [not] in a region like Asia, where there is this thing about saving face and a pronounced fear of failure.” This is different from Silicon Valley, which is unique in its acceptance of trying and failing as a natural part of building a business. As long as he or she works hard and is smart, an American

entrepreneur can go to a crowdfunding site and still save face if the target is not reached.

Scholars have however deemed crowdfunding to be *Shariah*-compliant, suggesting it could become an interesting opportunity for Muslim countries to explore. The World Bank’s 2013 report, ‘Crowdfunding’s Potential for the Developing World’, pointed to the early success of Eureeca, which helps small companies in the Middle East raise equity, and Shekra, an Islamic finance-compliant site which combines an incubator model with crowdfunding for Egyptian companies. “There is a bias towards real estate and equity in compliant [established companies], you also have some commodity funds, and so on,” Rushdi Siddiqui, Co-Founder and Managing Director of Azka Capital and Shekra board member, told industry site ‘Crowdsourcing’. “But in the area of venture capital, which is what the essence of Islamic finance is supposed to be about - partnership and risk-sharing - there is very little [activity].”

## Success Factors

When it comes to determining how successful a crowdfunding project will be, the quality of the project is only one factor. Ethan Mollick, Assistant Professor at the Wharton School of the University of Pennsylvania, found that equally important is the size and quality of the founder’s network, and whether the project has a connection to the founder’s geographic area.

“For entrepreneurs who seek crowdfunding, there are some clear lessons. First, project quality is important, and entrepreneurs should look for ways to signal preparedness. Social network ties have also been found to be important in crowdfunding,” said Mollick in his 2012 research paper, ‘The Dynamics of Crowdfunding’. “Second, appropriate goals are those that allow a founder to deliver a product on time; achieving significantly more funding than requested is rare. Most importantly, careful planning is required both to set these goals and to prepare for a crowdfunding success, which will entail a need to rapidly execute a promised venture.”

While smaller companies looking for crowdfunding may find there is more competition now as the funding method has become more popular, others may find there is more money to go around. As platforms are being set up to handle larger investments, the bigger guns in traditional finance are increasingly showing interest; US peer-to-peer platform Lending Club spent around USD1.5bn last year, and has among its directors former US Treasury Secretary Lawrence Summers and ex-Morgan Stanley CEO John Mack. Last year, US hedge fund Eaglewood Capital sold some of its Lending Club loans in a USD53 million securitisation deal, essentially giving institutional investors exposure to SME loans for the first time. Of course, this is nothing in comparison to the funds handled by traditional financing outlets, but for an industry that is only a few years old, it is a flying start. \*

■ Jessica Furseth is a freelance journalist based in London.



# Personal data protection

*and* **impact on banks**



**BANKING HAS NEVER BEEN MORE** customer-friendly as the industry is responding to demands for round-the-clock access to services. But while customers are hungry for convenience, they are also unforgiving about security breaches. Regulators are tightening up data protection laws worldwide, but ultimately it is up to the individual banks to make sure they honour their customers' trust. What lessons can be learnt from best practices on data protection in developed financial markets?

■ ANNA PERRY

Over a billion people in the world are now active on social networks, according to the International Telecommunication Union, often choosing to use the likes of Twitter and Facebook to also interact with our banks.

**B**ig Data has never been so big: a whopping 90% of all the data in the world has been generated over the last two years alone, and the pace of growth is accelerating. Every day we collectively produce 2.5 quintillion bytes of data and according to software group Autonomy, the number is so big it is beyond comprehension. Each of us is putting more and more details out there about our habits and preferences: how we pay bills, which groceries we buy, where we go on holiday, and what we say to friends online. Over a billion people in the world are now active on social networks, according to the International Telecommunication Union, often choosing to use the likes of Twitter and Facebook to also interact with our banks.

Financial groups, trusted by customers to handle sensitive information, face fresh challenges when it comes to personal data protection in the age of the Big Data boom. Information about customers are no longer just collected over the counter and held on local servers; banks now collect data through mobile phone apps, social media, and transcripts from overseas call centres.

## Convenience versus Security

The reward from mining Big Data can be significant for banks who are able to provide exciting new features tailored to customer needs. People increasingly want to handle their finances with the ease they have become accustomed to from shopping online or checking train times on the go via an app. But while customers are keen on convenience, they are also worried about security. Plus, they want more transparency about how their personal data is collected and stored.

This was the conclusion in Deloitte's 2012 'Data Nation' report, which found that while 80% of the UK population is aware that data is being collected by organisations, 54% would like to see stronger laws, better safeguards, and

more anonymity in order to protect their data. Whereas people could care less about businesses collecting data about their food preferences, 81% object to being catalogued when the data concerns sensitive topics such as finance.

"The public's attitudes towards data used by organisations [are also driven] by the lack of understanding of what data is collected, how and where it is used, and what benefits they will receive," said Richard Hammell, Head of Deloitte's UK Analytics Business. "Safeguarding individual privacy will become a moral and ethical responsibility placed on all organisations, rather than just a legislative action for the government."

A lack of awareness of how companies will use the data they collect is the primary concern. However, 42% of those objecting to the practice do so because they feel their personal data is none of the companies' business. Lost data was only a concern for 12%, meaning the issue is not just a headache in terms of security, but also in regards to public relations. Having said that, failure to keep data safe is the ultimate sin for a bank, with 70% saying they would likely take their custom elsewhere if this happened.

UK banks are becoming increasingly aware of this, and they are taking pains to prevent data protection gaffes. This was not always the case, however: a 2013 study from consumer charity 'Which?' showed 116 legitimate complaints against Barclays Bank filed at the Information Commissioner's Office (ICO) in 2010, followed by 114 complaints against Lloyds Bank. The most common grievance was failure to respond to so-called subject access requests, where people want access to their own data. David Smith, Deputy Commissioner of the ICO said: "Getting it right on data protection does not just mean keeping data secure. [...] The law also gives individuals an important right to remain in control of their information. I want to remind banks of the need to take this obligation seriously, providing full responses in a timely manner."

Better training for bank staff has led to fewer human errors, supported by improved technology which means a company laptop left in a train can now be wiped remotely to prevent a security breach. Still, regulators are keen to safeguard banks' reputations: the UK's Financial Services Authority (FSA) is currently reviewing the cyber security practices of over 30 major financial groups in a study, which will be used to improve standards across the industry. "The Treasury is working closely with the Bank of England and the FSA [...] to ensure cyber risks are better understood and to promote cyber security in the finance sector," Greg Clark, Financial Secretary to the Treasury, told the House of Commons.

## New EU Rules and Cohesion

The UK Data Protection Act has been in place since 1998, prompted by EU guidelines which were launched a few years earlier. The EU is now working on an updated set of rules, the General Data Protection Regulation, which is expected to come into effect this year. Lawmakers in the 28 member states voted in favour of the framework in March, with further negotiations on the details expected to commence in June. A single law will ease administration among all countries which currently all have slightly different rules, resulting in an estimated 2.3bn in annual savings for businesses.

"The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data," said EU Justice Commissioner Viviane

Reding. “A strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation.”

While the details of the new law are still being worked out, the debate over its efficiency is already in full swing; the Association for Financial Markets in Europe (AFME) argued the law may make Europe a less attractive investment prospect for international companies because it would bind them to the regulations even if only a few of their clients reside in Europe. Both the AFME and the British Bankers’ Association (BBA) have expressed concern about the maximum fine of 2% of the company’s annual worldwide turnover in the case of a data breach, a sum likely to be vastly in excess of the actual damage. In an open letter to the UK Ministry of Justice, the AFME and the BBA questioned the suggestion that banks will not be able to charge for subject access rights, a process that can be time-consuming: “If the request involves restoring back-up data and searching through potentially tens of thousands of emails, this can take considerably longer than the forty-day timescale in place at the moment.”

Looking beyond the details, a key theme for the new EU rules is the call for companies to be fully accountable for their data processing. “In practice, this will entail establishing a culture of monitoring, reviewing and assessing your data processing procedures, aiming to minimise data processing and retention of data, and building in safeguards to all data processing activities,” Jane Finlayson-Brown, Partner at law firm Allen & Overy, wrote in ‘Computer Weekly’. Many banks have already responded to the new law by operating a need-to-know system for customer information, while others are establishing systems to comply with the incoming rule that relevant parties need to be quickly informed following a breach.

Banks will also need to ensure they collect explicit consent to process

customer data, rather than relying on assumed consent. A much-discussed element of the EU regulation is the ‘right to be forgotten’, which means individuals could demand an organisation erase their personal data unless there is a legitimate reason to keep it. “If you store personal data, consider the legitimate grounds for its retention; it will be your burden of proof to demonstrate that your legitimate grounds override the interests of the data subject,” said Finlayson-Brown. She also warned that

#### ORGANISED

#### SMALLER FINANCIAL PROVIDERS

will also find their size may not protect them: “A high-profile brand might mean that casual attacks are more likely, but organised criminals are willing to do fieldwork. They look past the first few results on Google, and target organisations that are less likely to go public about problems and who are less likely to pursue them to the courts.”

banks “may also face individuals who have an unrealistic expectation of their right to be forgotten.”

#### Best Practice and the Recession Squeeze

While regulators are keen to get ahead in this rapidly expanding area, data protection has however been put on the backburner by many companies due to four years of recession in Europe and the US. “In today’s rapidly evolving threat landscape, businesses have fallen behind, their defences weakened and security practices dulled by a protracted period of tight budgets and truncated projects,” was the conclusion in PwC’s 2013 study ‘The Global State of Information Security’, which surveyed nearly 10,000 executives worldwide. “For many businesses, security has become a game that’s almost impossible

to win. The rules have changed, and opponents, old and new, are armed with expert technology skills, and the risks are greater than ever.”

The study showed 68% of respondents were at least somewhat confident that their organisations took information security seriously. However, only 25% reported that information security becomes involved in major projects at inception. Gary Loveland, Principal and Head of PwC’s Global Security practice, said: “Organisations that are true leaders in information security are much more likely to employ integrated approaches and frameworks that combine compliance, privacy and data usage, security, and identity theft.” Loveland recommended that businesses seeking to strengthen their security practices must have a comprehensive risk-assessment strategy. They must also properly understand their organisation’s information and the tactics deployed by adversaries who may want it. Also, finance groups wanting to be leaders in data protection must “embrace a new way of thinking, in which information security is both a means to protect data and an opportunity to create value to the business.”

This will mean a proactive stance on data protection, as even the world’s largest investment banks will admit they cannot stop criminals from getting through every single time. “Increasingly, efforts are turning towards effective preparation for, and response, to breaches. This levels the playing field with criminals going for the firms that cannot act quickly and decisively when things go wrong,” concluded Jon Pumfleet, Director in Deloitte’s Enterprise Risk Services practice. Smaller financial providers will also find their size may not protect them: “A high-profile brand might mean that casual attacks are more likely, but organised criminals are willing to do fieldwork. They look past the first few results on Google, and target organisations that are less likely to go public about problems and who are less likely to pursue them to the courts.”

## Keeping Track of Data

While the stigma of admitting to a data protection gaffe remains so high, it was perhaps surprising that the PwC study found only 40% could present an accurate inventory of personal data pertaining to customers and staff. How can you protect what you cannot locate? The study found 78% of financial services groups were confident that they have instilled effective security behaviours into their company, but only half have processes for handling data breaches by third parties. IT outsourcing providers were the source of 63% of data breaches in a recent study by Trustware, suggesting financial groups may need a reality check when it comes to keeping data safe when outside parties are involved.

The squeeze on data security budgets has not hit Asian banks to the same extent, the PwC study found, and a similar conclusion was reached by KPMG's report 'The State of Data Security and Privacy in the Indian Banking Industry'. Budget constraints were not the problem for data security in India, which, similarly to the region as a whole, benefits from notable investment in security. Other problems do however persist: "One of the most significant information security challenges highlighted by the banks is a lack of customer awareness on information security, and the threat from insecure customer endpoints," said Kunal Pande, Director of IT Advisory Services at KPMG. Pande expressed concern that the urge among banks to enhance the customer experience with convenient technology was at times undermining security.

In all geographies, the emergence of mobile devices, social media and cloud computing is presenting a new challenge for data management. The worrying conclusion is that technology adoption is often moving faster than security: "These new technologies are often not included in overall security plans," said Loveland, pointing to a study that found 88% of consumers use a personal mobile device for both private and work purposes, but only 45% of companies



## FINANCE GROUPS NEED TO WORK

with their cloud provider to make sure they remain compliant, as regulators may have rules on whether financial data can be stored across borders. But as long as banks have thorough processes for vetting cloud providers, there is no reason to think external storage is any less safe than keeping customer data in the back office.

.....

have a security strategy to address personal devices in the workplace. "Just 44% [of financial groups] have a mobile security strategy, while strategies for the cloud and social media clock in at less than 40% and lag the adoption rates of the technologies themselves."

## Cloud and Opportunity

As regulators are poised to clamp down on financial groups found to be slacking on data security, banks cannot afford to let this issue slide. "How well banks respond [to regulation] by building more flexible data management frameworks to implement new reforms, while also containing overall costs, will have profound implications for their competitive position in the marketplace," concluded Ernst & Young's 'Global Banking Outlook' report for 2013-14.

While the cost of change may be a bitter pill for many, investment will have

the positive side-effect of improving organisational effectiveness and customer service. "As banks consider the investment, potential revenue opportunities should be factored into the decision. Other industries, retailers in particular, have a strong track record of using customer analytics to interrogate data and provide more targeted offerings. We expect to see more banks follow this path and treat technology as both an enabler and a differentiator," said Steven Lewis, Lead Analyst in Ernst & Young's Global Banking & Capital Markets Centre. "Given more demanding customer requirements and expectations, banks will struggle to deliver improved service levels and pay for them through better cross-selling, without front-to-back technology changes."

Outsourcing data storage to cloud providers remains a controversial subject from a security perspective, with banks traditionally opting for so-called private clouds rather than handing over sensitive data to be stored externally. But this is starting to change as the cloud becomes safer, not to mention that external cloud storage can represent significant savings for banks.

Finance groups need to work with their cloud provider to make sure they remain compliant, as regulators may have rules on whether financial data can be stored across borders. But as long as banks have thorough processes for vetting cloud providers, there is no reason to think external storage is any less safe than keeping customer data in the back office. "A lot of people assume that if they keep data within the company then somehow they have more control than the cloud," said Greg Bell, Global Information Protection and Security Lead Partner at KPMG in the US. "But some of the more common cloud service providers have a few hundred people making sure data is well protected. It can be much better than what you see internally." \*

■ Anna Perry is a freelance journalist based in London.

# Data protection

## AND BANKS IN THE ASEAN REGION

### DATA PROTECTION REGULATION IS A HOT TOPIC

AMONG THE ASSOCIATION OF SOUTHEAST ASIAN NATIONS (ASEAN), WITH PROGRESS DRIVEN BY FINANCIAL GROUPS' OWN DESIRE TO IMPLEMENT BEST PRACTICES. BUT DESPITE IMPENDING INTEGRATION, THE ASEAN NETWORK CANNOT YET CLAIM COHESION ON DATA PROTECTION RULES, ESPECIALLY AS SEVERAL MEMBER STATES ARE ONLY JUST COMING AROUND TO THE NOTION OF A RIGHT TO PRIVACY.

■ JESSICA REE

**T**he data boom is a global phenomenon, but the drive for improving personal data protection is strongest in Asia.

Confidence on information security runs high in the region, concluded PwC's large 2013 study 'The Global State of Information Security', which found a stronger focus on security and more willingness to invest among Asian banks than their peers in Europe and the US.

As data protection regulation becomes a reality, the region's financial groups are assessing how they can collect and utilise data about individuals, and how this data is stored and transferred. "Asia's success in creating a culture of security

goes beyond spending. The region, in fact, boasts the highest number of self-proclaimed frontrunners," said Gary Loveland, Principal and Head of PwC's Global Security practice. This attitude is reflected in the fact that Asian banks and other corporations are increasingly considering information security from the very beginning of major projects, and are more likely to have security executives who report directly to the CEO. Banks now often have a dedicated information security officer; they make efforts to ensure data security is part of the company culture, and they regularly review their own approach to this rapidly changing issue. Added Loveland: "As for keeping up with new challenges, Asia rates highly for mobile security initiatives and cloud security strategy."



## Regulation and Self-Regulation

While financial groups in countries belonging to the Association of Southeast Asian Nations (ASEAN) are showing willingness to invest in data security, the region is also a leader on regulatory progress. Singapore and the Philippines saw their data protection acts passed in 2012, while Malaysia just passed an act last year and Indonesia is working on similar legislation now.

“Increasingly, the focus within financial services is on five key issues: regulation, cost, growth, technology and data, and change,” asserted Simon Topping, Head of KPMG’s Financial Services Regulatory Centre of Excellence in the Asia-Pacific

**This attitude is reflected** in the fact that Asian banks and other corporations are increasingly considering information security from the very beginning of major projects, and are more likely to have security executives who report directly to the CEO.

region. The various ASEAN countries are however at different stages of development; following KPMG’s 2013 report ‘Evolving Banking Regulation’, Topping pointed to how Singapore has already introduced misselling regulations, and proposals to improve consumer protection have been tabled in Indonesia and Thailand. “In Europe and the US, customer treatment is a major part of regulatory reform, and ‘treating customers fairly’ has become

an important underlying principle. In Asia the focus has so far been largely on misselling, on customer suitability and on investment products, but it seems inevitable that this agenda will be broadened over time.”

The ASEAN region has become the world’s most active in terms of new privacy developments, concluded Graham Greenleaf, Professor of Law and Information Systems at the University of New South Wales. Having said that, each nation is currently emphasising different aspects. Writing in the ‘Privacy Laws & Business International Report’, Greenleaf asserted that while the ASEAN countries are all working on regulation around the same point in time, these afford “very different strengths and weaknesses in the protections they give to data subjects”, and consequently the different laws present major compliance challenges for international businesses.



As banks struggle to deal with a multitude of regulatory requirements across several countries, one option is to apply a more unified and proactive approach to regulation within the company. "While experience seems to appear that many banks and financial institutions address regulatory issues 'as they come' and in a serial manner, the regulatory compliance challenges could be addressed by an 'optimised' parallel approach, which takes advantage of common business and processing traits across multiple regulations," concluded Nicholas Lim, Regulatory Compliance Head of IBM's Banking & Financial Markets Centre of Competence. "Banks need to [...] move from a regime of unique compliance initiatives for each new regulation, to a more sustainable, cost-effective, integrated framework capable of addressing current and emerging mandates," wrote Lim in 'Asian Banking & Finance'. "The process needs to be sufficiently scalable and responsive to address additional requirements. This is simply because regulations are changing all the time, and new regulations might be in force or new requirements are constantly being implemented by various regulators."

### Malaysia and the Philippines Echo the EU

After a lengthy delay, Malaysia's 2010 Data Protection Act came into force last November. Companies had only three months to comply with the first phase of implementation, however, a deadline that has been criticised as unrealistic. "This is indisputably too short a time to work towards compliance. Failing to comply with the act would render these organisations liable to criminal penalties," said Abu Bakar Munir, Professor at the Faculty of Law at the University of Malaya, and adviser to the Government of Malaysia on data protection in the run-up to the act.

For banks, complying with the new regulation now means entering a registry, as well as implementing new principles such as customers' consent to data collection, the right to be informed about data processing, and the right for data to be kept private. "The Malaysian Act has a lot of similarities with the European Data Protection Directive," said Gupinder Assi, Counsel at law firm Bryan Cave in Singapore. Writing in 'Lexology', Assi pointed to a number of principles the two have in common, such as an obligation not to keep data for longer than is necessary, and to recognise an individual's right to access their own data. A violation of the Malaysian act could lead to criminal liability or result in fines or imprisonment. However, Greenleaf pointed out that the limits on use and disclosure are weak, as there are numerous exemptions throughout the legislation.



Similarities to EU laws can also be seen in the 2012 Data Protection Act in the Philippines. While the rules apply to people in the country as well as foreign companies handling data about local residents, the act does not cover data concerning people who are citizens of foreign jurisdictions. Consequently, the European Commission is unlikely to add the Philippines to its list of countries it deems as having adequate safeguards for personal data, concluded Assi. An entry on this list would open the door to simplified data exchange between the Philippines and Europe, presumably a key reason for emulating EU regulations in the first place.

The Philippines does not require companies to register with any authority to comply with the act, but banks have to designate a data protection officer in charge of compliance. Securing permission for data collection and storage is a key requirement, along with the right of individuals to delete incorrect information. Added Abu Bakar: “An interesting point is that the law gives a right to the data subject to be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorised use of personal information.”

### **Singapore and Indonesia Take International View**

The 2012 Singapore Data Protection Act gives companies two years to comply with the new rules, which will apply to all companies handling data within the country. Similarly to the EU, the Singapore act mandates banks to only transfer data internationally if the recipient country has adequate rules in place. The right of individuals to control data being kept by companies applies also to the Singapore act, but Greenleaf noted a number of concerns: “There is limited extra-territorial operation for processing actions with a ‘Singapore link’. [The act] does not apply to the public sector. There are exemptions in relation to collection, use and disclosure for news organisations in relation to news activities, but these



**While Singapore, Malaysia and the Philippines** are the ASEAN nations in the lead on personal data protection, Indonesia is also taking notable steps. 2012 saw the initiation of a law on electronic transactions, which adds an element of privacy and a requirement to notify in case of data breaches.

only apply to organisations declared to be news organisations by the Minister for the purpose of this act. So there is potential for this legislation to be abused to further limit freedom of speech in Singapore.”

While Singapore, Malaysia and the Philippines are the ASEAN nations in the lead on personal data protection, Indonesia is also taking notable steps. 2012 saw the initiation of a law on electronic transactions, which adds an element of privacy and a requirement to notify in case of data breaches. “The absence of comprehensive data protection legislation in Indonesia is believed to have contributed to trading of personal data by insurance companies, banks and mobile phone service providers,” wrote Greenleaf in the ‘Privacy Laws & Business

International Report’, in an article co-authored with Sinta Dewi Rosadi, Law Professor at the University of Padjadjaran, Indonesia. “These laws are of somewhat limited scope, applying only to ‘electronic system operators’ and to actions ‘through electronic media’, somewhat similar to China.”

Indonesia’s law on human rights incorporates a right to privacy, which is becoming an increasingly relevant factor among ASEAN countries. “One impetus [for data protection regulation] comes from the international demand of partners of Indonesia in economic cooperation, including in ASEAN and the Asia-Pacific Economic Cooperation (APEC), and generally to further Indonesia’s strategic position on international trade including electronic commerce,” concluded Greenleaf and Rosadi.

## Harmonisation Plans

Brunei and Vietnam are expected to follow suit with their own data protection legislation, and Thailand currently has a personal data protection bill under review. The next landmark event will be the ASEAN Economic Community, with the lofty goal of economic integration for the region by 2015. If successful, this could result in potential harmonisation of data protection regulation among members. "Given this ambitious commitment, ASEAN member states should consider the regional integration of its respective data protection legislation, and to what level it may achieve the desired level of regional adequacy between them," Noriswadi Ismail, Co-Founder and Managing Consultant of QC, a data protection boutique consulting firm in Kuala Lumpur and London, wrote in his 2013 book, 'Beyond Data Protection'. This may include the advancement of cross-border electronic transactions through mutual recognition of foreign digital signatures, suggested Noriswadi, who also wants to see the establishment of an ASEAN data protection supervisor.

While the ability to move data easily and securely within the ASEAN partnership has clear benefits for the countries involved, a further key motivator for establishing a standard would be to ease interaction with Europe. EU data protection laws mean companies cannot move personal data outside of the European Economic Area unless certain protections have been put in place, and right now only a handful of countries are on the list of countries deemed to have adequate data protection. APEC countries operate a voluntary certified system aimed at ensuring consistency when personal data is transferred from one member to another, but a more streamlined system in the ASEAN sector would undoubtedly ease the process for global financial interactions.

"Singapore's participation in the development of tools for the APEC Cross-Border Privacy Rules system runs parallel to its efforts to develop



**APEC countries operate** a voluntary certified system aimed at ensuring consistency when personal data is transferred from one member to another, but a more streamlined system in the ASEAN sector would undoubtedly ease the process for global financial interactions.

a regime of binding corporate rules under Singapore's new data protection regulations," said Rosemary Lee, Counsel at Pinsent Masons MPillay in Singapore. "A primary impetus for adopting data protection law in Singapore is economic, and this new data protection regime is intended to enhance Singapore's reputation as an e-commerce and cloud computing hub."

## Culture and Privacy

While awareness on the topic of data protection varies widely among banks in the ASEAN region, the overall consensus among observers seems to be that the topic is being taken increasingly more seriously. The variation in attitudes between countries should not come as a surprise, said Masami Kashiwagi, Senior Analyst at research house Forrester, as the



concept of 'right to privacy' is relatively new to large parts of the region. "Some senior people have admitted to me that their organisations have not traditionally taken data privacy issues terribly seriously within their Asia-Pacific operations. But in a clear sign that this is beginning to change, governance risk and compliance practitioners are starting to see increased demand for their services, from both government and business sectors."

Technology adaptation among banks across the region is increasing in tandem with increased awareness of data regulation, said James Hatcher, Head of Regional Business of IT services group Seeburger in Malaysia. Writing in 'Asian Banking & Finance', Hatcher pointed out how this is particularly applicable to data exchange and communication technology, areas which traditionally have been under-invested and over-complicated by the financial groups themselves. "Banks are facing the challenge of collecting data transactions across a number of processes and complying in accordance with multijurisdictional requirements. Currently, banks tend to miss more than 80% of data in the form of files that need to be transferred across secured data transmissions systems," said Hatcher. "As part of any regulatory compliance and engageability, data needs to be tracked, traced and have the compliance department alerted."

As the laws of each ASEAN jurisdiction have been produced in response to local sensitivities to culture and politics, planning a region-wide approach to data privacy

compliance remains a challenge. Peter Bullock, Partner at law firm Pinsent Masons, commented how the lack of experience among Asian regulators, considered relative to their EU counterparts, is both a positive and a negative when it comes to developing systems: "While this [inexperience] makes some of the regulators less interventionist, it also means that they are often less predictable than their western equivalents. This all goes to uncertainty of the risk profile for data protection in individual jurisdictions."

While progress is quick, the fact remains that personal data protection regulation in ASEAN countries is still a relatively new concept. Similarly, local banks are less experienced in considering factors such as personal privacy and cross-border transactions, commented Noriswadi in 'Beyond Data Protection'. "The biggest challenge for ASEAN is that data protection is a new law. It requires maturity of governance, implementation and enforcement between the member states. The different cultural demographics, its historical legal systems and legislative influences and political enthusiasm differ." But having said that, Noriswadi is optimistic that ASEAN nations will benefit from a unified approach to data protection regulation, to the extent that the struggle to establish cohesion will ultimately be worth it: "So much so, ASEAN should be together to lead data protection irrespective of these hybrid differences." \*

■ Jessica Ree is a freelance journalist based in London.



## Case Study

## BBVA: LEADING IN PERSONAL DATA PROTECTION

**AS ASEAN INTEGRATION HERALDS TOUGHER COMPETITION,** AMBITIOUS ASEAN BANKS CAN TAKE LESSONS FROM GROUND-BREAKING BANKS THAT HAVE CONQUERED OTHER LANDSCAPES, LIKE BANCO BILBAO VIZCAYA ARGENTARIA. NOT ONLY A FRONTRUNNER WITH INNOVATION IN CLOUD COMPUTING, REVOLUTIONARY ATM DESIGN, AND INTUITIVE DIGITAL BANKING ASSISTANTS, THE GLOBAL SPANISH BANK MAINTAINS A STEELY FOCUS ON PERSONAL DATA PROTECTION, BECAUSE SECURITY REMAINS AT THE HEART OF CUSTOMER TRUST.

**B**anco Bilbao Vizcaya Argentaria (BBVA) has its house in order when it comes to personal data protection and security, but the multinational Spanish bank is also an industry leader in innovation. It is the successful co-existence of these two factors that makes BBVA interesting; the bank has seemingly succeeded in pushing innovation without compromising safety. This is a major challenge for the industry, where banks face a competitive landscape with demanding customers drawn to the convenience of apps and remote access, albeit with the corresponding security headache in a tightening regulatory landscape.

BBVA recently started using the Google cloud for data storage, an announcement which made headlines as financial groups have traditionally avoided placing sensitive data in communal data centres, cloud or otherwise. BBVA has adopted Google Apps for Business, a web-based suite of collaboration and communication products, in a deal which was a coup for Google by providing a brilliant case study for further pushes into the banking sector.

But its foray into cloud is just one event in its long history. Founded in 1857, BBVA services 50 million people with retail banking services, plus investment banking, asset management, and insurance. The leader in the Spanish market, BBVA is also the largest financial group in Mexico, with a significant presence in South America and the US Sunbelt. Present in 32 countries globally, BBVA's subsidiaries include Garanti Bank in Turkey and CITIC in China.

### Into the Cloud

Interestingly, BBVA explained the move to cloud computing as being not about saving money, but an effort to keep up with technological advancements. Carmen Herranz, Director of Innovation at BBVA, told the BBC: "The main goal is to promote innovation and decision-making and increase productivity. We are in a challenging market and need to make faster and more accurate decisions."

The move will see BBVA using Google's collaboration tools, including a social network-style intranet aimed at improving communication and exploring new ways of working. "With Google Docs, for example, we are excited about the real-time collaboration benefits, and we expect to increase productivity by removing the need to constantly update different versions of a document," said José Olalla, Chief Information Officer (CIO) at BBVA. "We are developing our new global intranet [to become] a place where all employees will be able to share, contribute and manage knowledge globally."



The increasing mobility of the bank's 110,000-strong workforce is another motivator, as BBVA explained how its data storage needs have changed as employees are increasingly accessing company data on smartphones, tablets or laptops at home or on the road, via the internet. Cloud access is also more efficient for BBVA because it allows the bank to buy more or less storage as needed; banks owning their own storage capacity rarely use even half.

By eliminating excess capacity, Google says its corporate customers habitually make cost savings of 50-70% when switching to the cloud. "It means a lot to us that BBVA, one of the largest financial institutions in the world, has decided to migrate to Google Apps," said Sebastián Marotte, Vice-President of Google Enterprise EMEA. "It shows that cloud computing is now a reality, and leading organisations are already realising its potential to transform their business."

BBVA's cloud deal is remarkable because of the bank's decision not to use a private cloud, instead choosing to spread its data across Google's public cloud network. This is a solution previously perceived to be less secure, but technology experts claim fears are exaggerated because large, professional cloud providers are likely more knowledgeable on data security than an individual bank. Still, BBVA has chosen to start by transferring only its internal communications data to the cloud, leaving customer details and vital banking systems out of it. This also means the bank remains compliant with regulatory requirements for data storage.

As the transfer to the cloud began, Herranz noted how the key challenge for the bank would likely be cultural, and BBVA had started training staff in how to use the new net-based tools. Employees have been encouraged to leave all old data behind in the legacy systems, said Herranz, as the bank "wants to start from scratch, [as we] don't want to carry across old behaviours."



## PRODUCTS

**BBVA HAS ADOPTED GOOGLE APPS** for Business, a web-based suite of collaboration and communication products, in a deal which was a coup for Google by providing a brilliant case study for further pushes into the banking sector.

## Cloud Diligence

As an innovator in a conservative industry, BBVA's decision to trust its data to the cloud may potentially trigger a slew of similar moves from peers. "I know from my contacts in other banks and other sectors that almost everyone is somehow looking at this," Olalla said to 'American Banker' following the bank's cloud move. But, he added: "In terms of time they are far behind us." Having said that, if peers see this working out well for BBVA, a precedent may have been set for less innovative banks to follow suit; the cloud option could mean notable savings in a banking environment still affected by the recession. BBVA has been reluctant to say the move will lead to redundancies for IT staff at the bank, although using cloud solutions will lead to fewer desktop-installed IT licences. "The idea here is not cost savings, it is innovation and transformation; we want to change the way people work," asserted Olalla.

BBVA's legal teams spent months working with regulators in various jurisdictions to make sure the cloud move happened within the remit of data protection regulation, not to mention the full year spent assessing whether Google's cloud system was sufficiently secure to be the right choice for the bank. Concluded Olalla: "Google meets all the security standards in the world, specifically the safe harbour standards. The way they manage the storage of data is to cut information in pieces and store it in different data centres around the world, which makes it impossible to access."

Google keeps the specific details of its data security procedures secret. However, it is known that customer data is scrambled using an algorithm, and stored in separate chunks in data centres across different geographical locations. BBVA also meets with Google once a month to discuss progress, which the bank has asserted has met expectations despite initial concerns whether online video conferencing would be of sufficient quality. This has been an issue for companies going to the cloud in the past, when internet connections were less reliable than they are now.

### International Security Focus

Looking beyond the cloud initiative, BBVA employs rigorous security procedures for all its data. Online access is guarded by electronic, physical and procedural safeguards, each tailored to comply with regulation pertaining to individual countries. Information is encrypted during transmission, meaning only authorised individuals can read it. The bank uses email to communicate with customers, but advises people to use the phone, post or branches for highly sensitive information due to the lack of encryption of standard email. So-called browser 'cookies', where information is stored during online visits for the purposes of convenience and tailoring, expire after each login session, again combining convenience with security.



The current high standards for data protection are a result of an overhaul in 2009, when BBVA became the subject of nine disciplinary cases from the Spanish Data Protection Agency. Following this, the bank created a dedicated Global Fraud Risk Unit, tasked with establishing and coordinating policies across the global operations: "To prevent and mitigate fraud in all the businesses and geographical areas of the group, the unit defines strategies, undertakes initiatives and develops actions within the framework of the bank's corporate principles, based on a global management model." BBVA also implemented a zero tolerance attitude to fraud, and 2009 saw the launch of a five-year Information Security

Master Plan for the company, aimed at bringing information security into the heart of the organisation's culture.

Operating in 32 countries, BBVA finds itself needing to consider a vast number of differing regulatory environments, as well as national and international best practice standards. The bank itself is incorporated in Spain and authorised by the Bank of Spain; it complies with the EU Electronic Commerce Directive; meanwhile the bank's registered office is in the UK and subject to limited regulation by the Financial Services Authority. The bank also complies with the US anti-money laundering regulations. BBVA clearly explains how it uses customer data: "Companies in the BBVA group will

**SERVICES****BBVA'S CONTIGO SERVICE STANDS TO**

**POTENTIALLY** replace branches altogether by combining people's need for a personal relationship with convenient banking. Contigo designates a personal advisor to each customer, allowing them to build a relationship via phone, video and internet. Consequently, all banking services can take place without the customer ever having to set foot in the branch.

use your information to manage your accounts, give you statements and provide our services for assessment and analysis, including credit or behaviour scoring, market and product analysis, and to develop and improve our services to you." BBVA also complies with the EU's requirement of only transferring personal information over national borders if the recipient can prove the same levels of protection. The exception to this may be to comply with anti-money laundering or anti-terrorism laws.

As international regulatory compliance can be costly and time-consuming for global organisations, BBVA Compass in the US employed the services of data integration software expert Informatica to help with the implementation of anti-money laundering procedures. "Informatica has enabled BBVA Compass to successfully pull data from a variety of disparate sources across the business for business intelligence and regulatory reporting purposes. The platform is easy to use, there are no issues with the performance, and the scalability allows BBVA Compass to add more sources quickly, including from newly acquired business should it be necessary," said Tapan Shah, Project Executive at consultancy Crowe Horwath and leader of the Informatica integration project.

**Digital Future**

"Over the past decade, BBVA has worked hard to become more customer-centric and match its offerings to customers' needs. Given the pace of technology change, customers' rising expectations and the digital disruption those forces cause, innovation is a critical part of the role of eBusiness and channel strategy executives," said Benjamin Ensor, Analyst at research house Forrester. "BBVA clearly has an innovation budget and team most eBusiness and channel strategy professionals can only dream of. [...] But what makes it stand out is its determination to create better customer experiences. BBVA has embedded innovation at the heart of its strategy to become a more customer-centric bank."

Living up to this strategy, BBVA was one of the first banks in Europe to introduce online money management back in 2008. Now the bank is claiming headlines yet again with a

radical redesign of the automated teller machine (ATM). With help from San Francisco design consultancy IDEO, the new ATMs were developed after studying customers' behaviour, resulting in simple yet brilliant new features such as a shelf for putting down papers or cups of coffee. Most importantly, customers stand at 90 degrees to people waiting in the queue, preventing others from catching the pin code over their shoulder, as they are also shielded by a frosted panel. The award-winning design was further simplified by using one slot for inserting and withdrawing cards, monies and receipts, while a virtual teller named Hero guides people through the touchscreen experience.

Further initiatives from BBVA include Lola, an intelligent banking assistant working in a manner similar to iPhone's Siri. "Lola is a cornerstone of BBVA's customer-centric banking vision, which includes bringing the simplicity and reassurance of in-branch banking to the online world," said William Mark, Vice-President of Information and Computing Sciences at SRI International, BBVA's technology partner on the project. Lola not only understands language, but also builds an impression of the user's intent through conversation, explained Mark, as people usually need a couple of sentences to express what they want to do. Lola will also make personalised recommendations, similar to a human assistant, and leads the customer through a banking experience where the structure and displayed information are tailored to suit the customer's preferences.

BBVA's Contigo service stands to potentially replace branches altogether by combining people's need for a personal relationship with convenient banking. Contigo designates a personal advisor to each customer, allowing them to build a relationship via phone, video and internet. Consequently, all banking services can take place without the customer ever having to set foot in the branch. BBVA's Contigo and Lola initiatives were highlighted as best practice examples in Accenture's report 'Digital Relationship Management'. "Far from just handling complaints, digital relationship management uses data and analytics to understand and pre-empt customer needs, and offers targeted information to create more relevant and timely service messages," said Joydeep Bhattacharya, Technical Project Leader at Accenture. "Tools range from knowledge management, alerts, collaborative browsing and web chat, to 'social' customer service, virtual assistants and remote advisory services." Getting this right can improve a bank's customer services and sales, as well as reduce cost and boost loyalty.

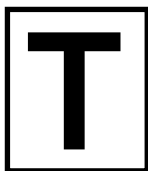
But at the end of the day, data protection remains the key. No innovation in the world will win over customers unless they trust the bank to keep safe what is shared in confidence. \*

■ Reporting by the *Banking Insight* Editorial Team.

**COULD STRINGENT COMPLIANCE** REQUIREMENTS BE A CATALYST FOR INNOVATION, RATHER THAN A COSTLY AND RESOURCE-HEAVY BURDEN? INSTEAD OF FEARING **BASEL III**, BANKS SHOULD VIEW IT AS AN AVENUE FOR REFORMATION WHICH COULD TRANSFORM PERFORMANCE AND PLACE THEM ON A STRONGER FOUNDATION FOR INNOVATION AND GROWTH.

# REFORM TO PERFORM

■ ECKART KOERNER



hough banks might view the advent of Basel III as an obstacle, it may in fact be the driver to challenge and spur them to consider more holistic reforms and innovations. Instead of viewing it purely from a compliance angle, Basel III could be the motivation for an overriding innovation agenda - one which will channel reform not only from a product and instrument perspective but possibly overhaul the complete business model of banks itself.

### The Malaysian Context

In the wake of the global financial crisis which erupted more than six years ago, the regulatory momentum driving forward has been steadfast. Regulatory pressure intensified with Basel III requirements beginning to come into force in the local markets, and banks

are feeling the heat. At the same time, the local regulator is introducing other guidelines seeking to strengthen areas of governance and risk management, signalling a need for transformation.

Basel III builds upon its predecessors, Basel I and II, focusing on strengthening capital and liquidity regulations to ensure a more resilient banking sector with minimised spillover effects to the real economy, due to an improved ability to absorb shocks from financial and economic stress. Key principles include higher minimum capital requirements focusing on better quality of capital, strengthened liquidity requirements ensuring liquidity in times of stress, improved risk coverage, constraints to leverage within banks, and build-up of capital buffers. Without doubt, the extensive coverage and heightened requirements appear intimidating and costly.



However, Malaysian financial institutions would be well-advised to consider Basel III as an opportunity to innovate and grow, rather than a barrier to performance. While the Malaysian banking market has become well-versed with Basel III and its requirements in recent years, the trepidation felt by banks with regards to perceived regulatory limitations hints that Basel III may still be viewed as a hindrance to business.

Yet, another look at Basel III and its impact on the market may unveil a different perspective, suggesting that heightened requirements do not necessarily mean an additional burden but may instead provide a trigger for all-encompassing innovation.

### **Spurring Innovation, Realigning Business Models**

The temptation to revert to minimal solutions or workarounds is understandable, where there may be motivation to do only what is required and to an extent that can minimally affect a bank's current operations and costs. However, this approach could be costly for long-term competitiveness and sustainability – and



While the Malaysian banking market has become well-versed with Basel III and its requirements in recent years, the trepidation felt by banks with regards to perceived regulatory limitations hints that Basel III may still be viewed as a hindrance to business.

stunt innovative thinking. Instead of designing a response to Basel III that aligns to their business model, banks may want to consider a proactive redesign and realignment of their businesses to ultimately lead to an optimal level of balance between stability and profit.

For each existing or newly innovated product and instrument, banks have to consider the impact of the offering to capital, liquidity and leverage. Along with a host of other parallel regulatory requirements running alongside Basel III, this becomes a multi-faceted conundrum during the design phase, all of which is challenging by the fact that these factors are not necessarily positively correlated. From an instruments' view, banks are already innovating to meet the new requirements, such as the recent issuance of the world's first Basel III-compliant Tier-2 subordinated *Sukuk* by AmIslamic. This liability instrument was engineered to incorporate the required characteristics of Basel III capital instruments into an Islamic context, in which the design of the *Shariah* mechanism itself was not without its own challenges.

# Impact

Banks will need to consider the impact of the agenda to achieve stable income on their business model, customer focus and product focus.

However, solutions such as raising capital and re-focussing business to achieve compliance instead drive up the pressure to perform and combat rising capital costs. Banks would need to consider fundamentals of the business to determine the viability of such measures. The key determinant to motivate the banks' actions will foremost be the capital cost of the bank or in other words, the return on equity. This is driven by the P/E ratio of the bank, where banks must strictly consider if their P/E ratio is sufficiently high to justify such actions and allows the bank its competitive edge, i.e. where capital costs are advantageous.

Even in the cases of good P/E ratio performance, banks must emphasise the continuance of their P/E ratio as its impact on capital cost remains of great focus. Banks will need to consider the impact of the agenda to achieve stable income on their

business model, customer focus and product focus. As the reduced capital cost will give the bank breathing room in this time of high capital requirements, the sustainability of the business model established is critical to its long-term agenda and the ongoing continuity of that benefit.

## Liquidity Concerns Driving Innovation

The liquidity perspective is another key area of concern in the Malaysia market. According to the European Banking Authority 'Report on Impact Assessment for Liquidity Measures', impact assessments performed in other markets suggest that liquidity requirements are not expected to have a material detrimental impact on the stability and orderly functioning of financial markets, the economy and the stability of supply of bank lending. However it found that banking business models that are more

diversified will be better adapted to cope with regulatory liquidity requirements than specialised banks.

In the case of investment banks for example, other deposits are more harshly penalised in comparison to retail deposits in respect to these requirements. This leaves investment banks at a disadvantage compared to other banks given that they are not able to access retail deposits, which are favoured and viewed as more stable by Basel III standards.



Investment banks will then have to reconsider several possibilities that are available to them; should they be restructuring their liability side and/or reconsidering their focus on the asset side? A variety of concerns ensue with their liabilities, more prominently the consideration of funding cost implications from the restructuring of funding in favour of bonds instead of wholesale funding. On the asset side, we are bound to see a shift to more fee-based revenue as opposed to interest-based revenue to ease pressure on the requirements.

Insights derived from other markets with inequalities between each customer segment under Basel III considerations should encourage the local Malaysian banks here to carefully consider a more thorough response in the bank. Instead of laboriously pondering over more small-scale and direct solutions of improving their compliance with new regulations, a more comprehensive revisit of their business model and business strategies may prove more fruitful.

### Limitations on Innovation

Despite that, when it comes to reform or innovation opportunities, these understandably do not happen without challenges or resistance. The sophistication of risk areas in the bank plays a huge role in its feasibility and in barriers to the innovation agenda. Banks may be limited to restricting solutions if capabilities in risk and capital management are not of a standard that can facilitate a more holistic transformation.

**Data systems and quality struggle to sustain a parallel rise in capabilities to the ever-increasing expansion of a bank's data requirements for risk management.**

Foreign banks from large banking groups that are established locally in Malaysia may be able to leverage on the insights and strategies witnessed and employed first-hand by their parent and other subsidiaries in other markets. Similarly, large regional banking groups could also be better equipped with resources in risk and capital management.

Data management remains a prevalent issue for banks in this time of reform and emphasis on ongoing innovation. Data systems and quality struggle to sustain a parallel rise in capabilities to the ever-increasing expansion of a bank's data requirements for risk management. Furthermore, data requirements are not often a one size fits all solution; various competing parties demand different sources and aggregations of data, leaving limited opportunities for leveraging on existing outputs. The advance of the bank can thus face constraints placed by data capabilities, and this undermines the effectiveness of risk management as a whole.



### OPTIMISE

**Another critical area** is the effective implementation of risk-based performance management within the bank to optimise capital consumption. In the Malaysian market, mostly larger banks and foreign banks have taken significant strides in integration at this juncture and reaped more concrete benefits.

Another critical area is the effective implementation of risk-based performance management within the bank to optimise capital consumption. In the Malaysian market, mostly larger banks and foreign banks have taken significant strides in integration at this juncture and reaped more concrete benefits. For other banks that may not have the resources for effective implementation, this represents an uphill battle where they may have diminished clarity in the linkage between strategic planning, risk and capital management.

Innovation is bound to be part-and-parcel of every bank's agenda over the next few years. Regardless of their reservations, they need to embrace this era of reform in order to stay competitive and emerge ahead of the crowd. In the end, the final goal of a more stable, forward-looking and resilient banking sector remains the same. \*

■ Eckart Koerner is an Executive Director and part of the Financial Risk Management Services of PwC Malaysia. He has extensive experience in risk management for financial institutions. In particular, he focuses on topics related to integrated risk management, Basel II & III projects (risk measurement & management, regulatory compliance), risk measurement tool validation and capital management & optimisation as well as comprehensive stress testing implementation.

# M

obile technology is transforming the banking landscape as more telecommunication services providers and network operators rush to capitalise on the growing market for mobile services. To avoid becoming bit-part players in the future, banks today are looking to adopt a solid and flexible strategy to support mobile banking and cashless payments.

Looking deeper, today's mobile usage is not just growing, but it is also deepening as advanced technology becomes more accessible and affordable. Computing power, operation scalability, and modes of user interactions of mobile devices are constantly being enhanced, driven by the consumers' demand for personalisation.

Therefore, when mobile technology is used as a mode of accessibility to financial services, customers expect the same level of personalised and contextual engagements. In order to begin to meet consumer expectations, banks need to enable mobile transactional banking and engage the consumers on their own terms.

### Enabling Transactional Banking on Mobile

Investing in transactional capabilities on mobile is the most crucial and first step that financial institutions should look at. This is because mobile platform is where a customer's enquiries can be converted into sales, thus generating revenue and driving immediate returns on financial institutions' mobile investments.

For instance, after extensive research on a financial product or service on their smartphone, it is highly unlikely that consumers will travel to their nearest branch to make the transaction immediately. However, with transactional banking functions available on their smartphones, consumers can apply for a product or service through their mobile device and complete the transaction instantly. Hence, the bank stands a better chance at closing a sale, especially with consumers who are already connected.

### Engaging Consumers on Their Own Terms

Traditional banking models with fragmented channels simply are not a good fit for consumers' evolving needs and changing modes of behaviour. Accustomed to sourcing for information themselves and taking advantage of collaborative networks and tools, consumers, especially those from Generation Y, tend to expect more integrated services from banks regardless of channels.

Banks need to engage consumers on their own terms and deliver a differentiated customer experience. Meeting consumers' ever-changing expectations means engaging them in a real dialogue founded on social interplay and personal trend monitoring.

A comprehensive banking platform of today needs to provide not only banking insights and the security to build long-term trust and lasting relationships with consumers, but to also address the following issues: (page 56)



## Engage

Banks need to engage consumers on their own terms and deliver a differentiated customer experience. Meeting consumers' ever-changing expectations means engaging them in a real dialogue founded on social interplay and personal trend monitoring.



# Embrace the Mobile Revolution

BANKS MUST LEVERAGE ON MOBILE TECHNOLOGIES TO ENGAGE CUSTOMERS ON THEIR OWN TERMS AND CONQUER THE GROWING MARKET FOR MOBILE FINANCIAL SERVICES, OR RISK BECOMING IRRELEVANT IN A NEW GLOBAL LANDSCAPE WHERE CONSUMER DEMANDS AND EXPECTATIONS FOR PERSONALISED SERVICE ARE CHANGING IRREVOCABLY.

■ VENKY SRINIVASAN

- Integrate online platforms with mobile capabilities to help engage the consumer via the banking portal, supply assistance and generate leads;
- Personalise user interfaces and notifications to reflect individual preferences and drive customer loyalty; and
- Invest in social media to build engagement through advertisements, dialogues, and personalised services.

### The Need for Contextual Banking and Getting It Right

As the expectations of mobile customers increase, so does their impatience with blanket marketing, spam and generic advertising. To truly get the most from mobile banking, financial institutions must be able to address their consumers in context.

- Banks must not only cater to the consumer's mobile needs, but also integrate the context of each interaction into their service offerings such as from the perspectives of consumer's past behaviours, established preferences and their geographical location.
- Integrated, multichannel call centre assistance and product-focused social-media updates can be key tools in building context-specific interactions with retail banking consumers. Where the higher end of the retail segment and private banking consumers is concerned, contextual engagement involves connecting a consumer directly to their relationship manager, or offering shopping discounts based on proximity to a service or location.

Effective contextual banking relies on accurately predicting the consumer's needs, priorities and next moves based on their past interactions. It is about being able to effectively recognise

the best methods of engagement with different consumer bases. In this case, behaviour simulation is the key to engage consumers in the correct way at the right time by giving banks the insights they need to enhance services based on consumer sensibilities.

### Contextual Banking and the Digital Wallet

A key element of contextual banking on mobile is the digital wallet. In Europe and North America, consumers typically see the digital wallet as a digital expression of the physical wallet, consolidating payment options, coupons and vouchers. They expect the wallet to offer them new capabilities such as Personal Financial Management (PFM) tools.

In many rural and emerging economies such as in Africa and the Philippines, the digital wallet has also gained acceptance as the preferred option for financial transactions. It becomes the backbone of financial inclusion, institutionalising account opening and revolutionising microfinance.

The real-time and context-enhanced mobile banking is set to play an increasingly important role in transforming consumer experience and building brand loyalty. The following are some examples of how contextual banking works on mobile in practice.

- In the scenario of a consumer who is in the market for a new car, the contextual engagement could first be portfolio-driven. For instance, the bank could offer the consumer a mobile app that walks them through the process of loan application in real time as this has the potential to enhance customer satisfaction and loyalty and to accelerate the transaction.
- Secondly, contextual banking could occur from a location-driven perspective. If the bank can identify when the consumer is at a car dealership, it can instantly issue the

loan offers needed to encourage the purchase.

- Contextual banking could also improve a consumer's point-of-sale experience.

Take a consumer who buys coffee on her way to work every day. The coffee shop that supports mobile payments can intelligently engage contextual mobile banking to improve her experience and enhance loyalty.

For instance, when she uses her mobile to make the payment, her balance is adjusted in real time allowing her to instantly track her monthly coffee expenditure on her PFM application. When she visits the same outlet the following day, or even another outlet of the same coffee chain, her location and transaction preference will be automatically detected for instantaneous mobile order placement and billing.

### The Time is NOW

With the global economy showing signs of gradual recovery, now is the time for financial institutions to be proactive and grasp the huge opportunities that mobile banking presents.

Banks still have an advantage. While new mobile financial services providers have seized the initiative when it comes to mobile banking, banks still own the financial ecosystem and have the advantage of existing consumer relationships and higher levels of trust.

Banks that are able to quickly develop and deliver smart, contextual mobile banking products and services stand not only to achieve phenomenal growth, but also to create even deeper and more productive customer relationships than ever before. \*

■ Venky Srinivasan is Vice-President, Sales, Asia Pacific & Japan, for the Financial Services Global Business Unit of Oracle Corporation. He is responsible for driving sales across the identified strategic markets for banking and insurance.



Being committed to your needs.

Being on this journey together.

**Thank you.**



To our customers, shareholders and business partners: thank you.

Thank you for choosing us as your preferred financial partner in Asia. Your support has made us the leading financial services group in Asia and one of the world's strongest banks\*.

We are honoured to have taken this journey with you, one that has spanned over 53 years, across 2,200 offices in 20 countries, bearing over USD171 billion in assets.

As a global bank that has grown in Asia, we have seen a remarkable economic growth in the region and are proud to have fueled the transformation for over 53 years, as a participant and not just a witness.

With your encouragement and contribution, we are living our mission of Humanising Financial Services Across Asia.

We are bridging worlds in Asia by identifying the gaps in this complex and diverse, yet modern and ambitious market. Gaps between technology and people, progress and responsibility, values and growth, and ambition and possibilities.

And by closing these gaps, we're helping our customers constantly stay connected to opportunities across the region.

Because we believe that for everything that keeps us apart, there's always something that brings us together.

To us, this is humanising financial services. This is the future.

\*Source: Bloomberg Markets' Annual Ranking of the World's Strongest Banks

# PREDICTING FINANCIAL CRIMES

**PARTICULARLY WHEN IT COMES TO BANKS,** CYBERCRIMINALS LOOK FOR THE WEAKEST LINKS IN THE INFORMATION SUPPLY CHAIN, WHICH MEANS INSTITUTIONS CAN COME UNDER INDIRECT ATTACK EVEN WHEN THEIR OWN SYSTEMS ARE SECURED. FINANCIAL INSTITUTIONS CURRENTLY PRACTISE AN OUTDATED AND REACTIVE APPROACH WHERE THEY CONDUCT FORENSIC ANALYSIS ON THEIR DATA, SYSTEMS AND NETWORKS AFTER BREACHES HAVE OCCURRED. TO BE PROACTIVE, DECISION-MAKERS NEED TO BE EQUIPPED WITH ANALYTICAL TOOLS THAT WOULD BE ABLE TO DETECT AND PREDICT THE SEVERITY OF POSSIBLE ATTACKS BEFORE THESE OCCUR.

■ KEITH SWANSON

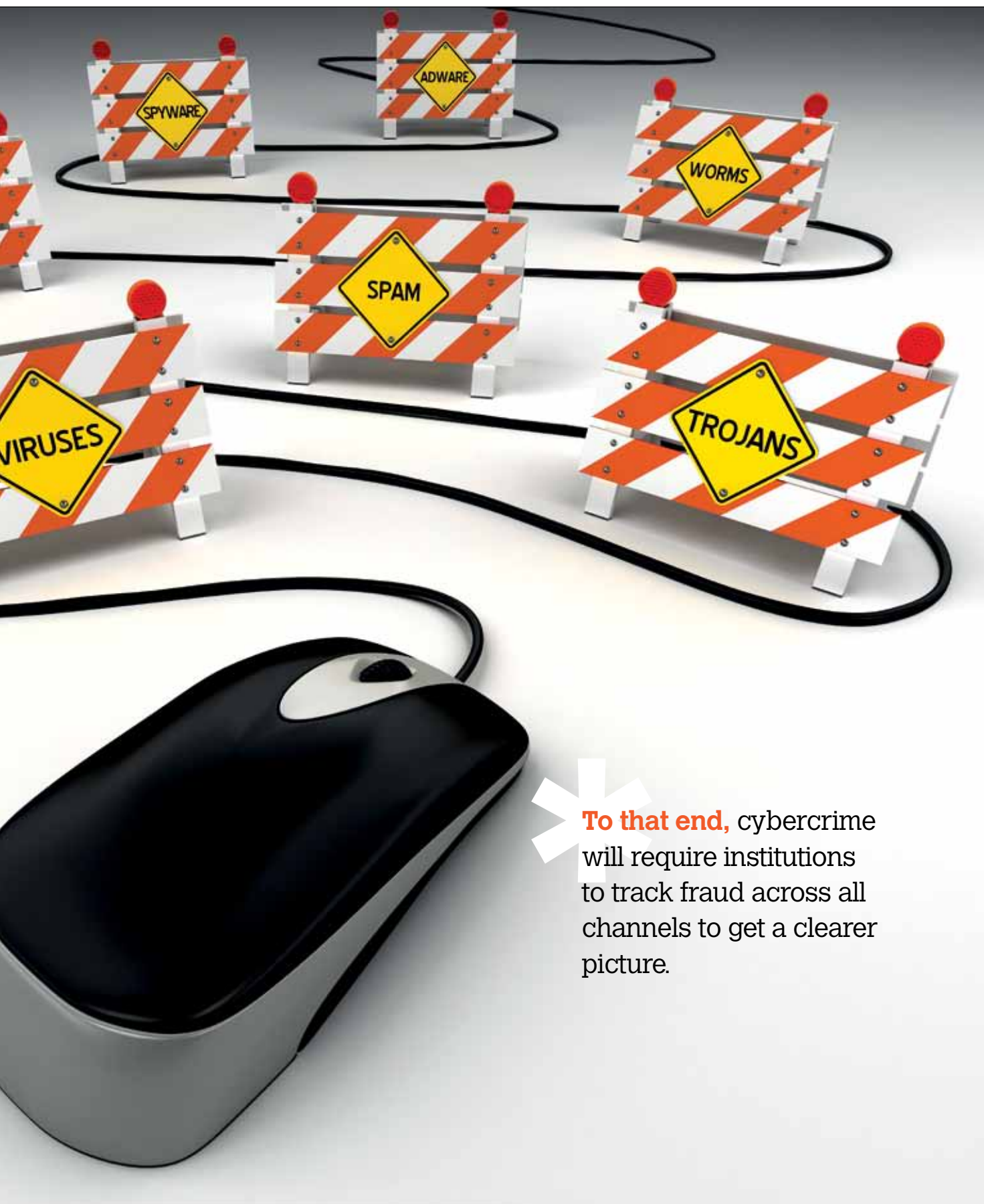
**T**he rise of the information society has provided a wealth of opportunities for financial services institutions to enhance services to customers through new channels. However, as they continue to innovate in finding and introducing new ways to reach customers, they simultaneously expose themselves to new risks. The opportunities and dependence on information and communications technologies (ICT) then come with an elaborate landscape of threats that are becoming increasingly complex. Cybercriminals are constantly searching for new ways to exploit weaknesses and are working to develop ever more sophisticated methods of attack.

The threat landscape comes with a convergence of offline fraud and online crimes. Particularly in banks, cybercriminals look for the weakest links in the information supply chain, which means institutions can come under indirect attack even when their own systems are secured. This is one of the rising complexities of cyber threats and the proliferation of such attacks would mean that banks can no longer

protect their customers by simply securing their own online assets. In a September 2013 report 'Cyberrisk in Banking' by Longitude Research with SAS, David Pollino, Senior Vice-President and Enterprise Fraud Prevention Officer at Bank of the West, said that organised crime groups will try to break into banks across multiple channels. It does not matter whether it is done online; they look for the weakest link.

To that end, cybercrime will require institutions to track fraud across all channels to get a clearer picture. "Many times, what you see in a single activity isn't that dramatic, but when you look at the total relationship and the total activity, you could then identify and link potential cybercriminals and prevent fraud in a proactive manner," said Dan Barta, Industry Consultant for SAS Global Fraud and Financial Crimes Practice. It is important that banks evolve how they perceive such problems – rather than focusing on vulnerabilities, banks should instead focus on looking for proactive remedies. Financial institutions currently live in a reactive world where they conduct forensic analysis on their data, systems and networks after breaches have occurred. This approach is becoming increasingly outdated and ineffective.





**To that end,** cybercrime will require institutions to track fraud across all channels to get a clearer picture.

**THE WEAPON OF CHOICE** HERE IS THE USE OF CYBER-ANALYTICS WHICH PROVIDES MANY TOOLS AND PROCESSES THROUGH STATISTICAL ANALYSIS AND MODELLING – WHICH CAN BE APPLIED TO FRAUD DETECTION, FINANCIAL MANAGEMENT OR HUMAN RESOURCES. THE NEAR-REAL-TIME ANALYSIS CAN SWIFTLY GENERATE ATTACK ALERTS WHILE SIMULTANEOUSLY REDUCING THE NUMBER OF FALSE ALARMS.

For instance, in early 2013, a highly coordinated attack involving people across some 20 countries took place where cybercriminals worked with local groups to manipulate financial systems using magnetic strips on debit and credit cards. This was conducted in just two separate attacks to steal USD45 million from thousands of ATMs around the world. While an ATM heist is an age-old crime, the methods deployed were wholly from the 21st century. The hackers firstly identified prepaid debit cards as their primary targets as they are preloaded with money instead of being linked to specific accounts, thus minimising early detection. Hackers then looked into the financial system's weakest link and infiltrated an unnamed Indian credit card processing company to steal information. They then increased or removed the withdrawal limits on the prepaid cards by infiltrating the National Bank of Ras Al Khaimah in the United Arab Emirates and the Bank of Muscat in Oman. Once the needed information was obtained, the cybercriminals executed the plan through global coordination where information was sent to local crews in about 20 countries around the world. They then used the data to programme the magnetic strips of cards in order to withdraw money on their local ATMs.

By December 2012, the local crews had used five account numbers to make 4,500 transactions worth USD5 million. By February 2013, these cybercriminals had used 12 accounts to make 30,000 transactions worth USD40 million. This 21st century ATM heist illustrates the growing complexity of new payment system threats. Banks need to understand their adversaries and anticipate new, sophisticated forms of attack, or new versions of old tricks. At the same time, banks must also work to ensure that their partners and stakeholders are secure as part of strengthening the entire supply chain of information to minimise attacks against the weakest links.



Consequently, there is a growing need for financial services institutions to venture into real-time fraud processing and tracking of transactional data. It is also important to better harness data analytics to make proactive decisions, especially in the ever-changing technology landscape. The weapon of choice here is the use of cyber-analytics which provides many tools and processes through statistical analysis and modelling – which can be applied to fraud detection, financial management or human resources. The near-real-time analysis can swiftly generate attack alerts while simultaneously reducing the number of false alarms. Time is of the essence and decision-makers need to be equipped with analytical tools that would be able to detect and predict the severity of possible attacks before they happen. This is done by monitoring activities; uncovering vulnerabilities, threats and patterns; integrating disparate data to find patterns and trends; and predicting future threats and attacks so proactive measures can be taken to protect their data and networks. With a technique known as predictive analytics, cyber-analytics also provide early recognition of anomalies in network traffic and uncover possible hidden relationships and behaviour patterns that might indicate low and slow attacks.



**Lack of shared information** among business units is also another key challenge to cybersecurity. Regardless of industry, organisations that do not sufficiently coordinate and monitor business processes will fail to uncover non-compliance with policies and regulations.

Analytics can be seen as contributing to a holistic view of an entire chessboard – where the pieces are located, both white and black. This holistic view significantly improves the coordination of cybersecurity efforts and produces metrics which provide a more accurate picture of those efforts. With that, financial services institutions would be able to better understand, use and protect their data, regardless of volume, condition, state or location. This leaves cybercriminals with little or no room to attack when institutions and their stakeholders have the ability to look three or even four steps ahead by finding the loopholes before the attacker does.

As a whole, it is important to note that the cyber domain is constantly evolving, providing both new opportunities and challenges for financial services institutions. To improve cybersecurity, financial services institutions must elevate the topic and address threats holistically to the highest levels

of the organisation in a manner they understand. In this effort, there is a need to firstly understand the threats – just like the likelihood and impact of cybercrimes varies, so should the responses to them. Secondly, data assets need to be leveraged on with advanced analytics. Like many organisations, banks have enormous amounts of data at their disposal which they can use with analytic tools to detect trends to proactively counter cyberthreats. Lastly, taking risk-based decisions is of utmost importance where elevation of a problem to an operational risk is required, from which better decisions can be made faster and in relation to the relative risk to the enterprise as a whole.

Lack of shared information among business units is also another key challenge to cybersecurity. Regardless of industry, organisations that do not sufficiently coordinate and monitor business processes will fail to uncover non-compliance with policies and regulations. This fact has played out time and again in headlines that describe fraud, theft, customer data breaches, and so on. The fallout can be costly and therefore, the purpose of governance, risk and compliance (GRC) programmes is to promote compliance with policies and applicable laws. This is effectively done with a GRC solution which is able to help institutions adhere to laws and regulations, as well as understand and manage risk exposures.

In the effort to meet the cybersecurity challenge, banks will be helped by evolving technologies too. New tools are rapidly being introduced to fill existing gaps in both reactive forensics, such as e-discovery solutions and proactive analytical tools, which can mine significant data sets to analyse patterns and support risk-based approaches to managing risk. The use of 'big data' is only valuable if it can be properly analysed and provide a sound basis for making better decisions. Implementing analytics can help financial services institutions better understand what, when, why and how threats can potentially have an impact on an organisation, and how they can determine the most appropriate action to meet the challenges ahead. \*

■ Keith Swanson is the Director of the Financial Crimes and Security Intelligence COE for the SAS Institute South Asia. Prior to joining SAS in 2010, Keith held a number of senior positions with a longstanding SAS customer in the financial services sector in the US. He also spent time in management, business process and analytics consulting with leading organisations including IBM Global Business Services.



# *Control* - Key to Cybersecurity

**Understanding and innovating the concept of control is essential to manage and mitigate risks for cybersecurity professionals in the banking industry**

■ AMMAR HINDI

# Control

The method to achieve that control requires a fresh approach that incorporates automation, integration and education.

**THE CONCEPT OF CONTROL HAS LONG BEEN A CORNERSTONE FOR** virtually every banking institution's cybersecurity team in their approach to dealing with threats. However, with cybersecurity professionals in banks finding themselves at an increasing disadvantage when defending their IT environments, it may be unrealistic to expect control over threats and outbreaks. Attackers are singularly focused on penetrating a bank's network to accomplish their missions. Yet the job of the defender has never been more challenging. As banking networks extend beyond the traditional perimeter to include endpoints, mobile devices, virtual desktops and data centres and the cloud, new attack vectors emerge. Furthermore, there are many fraud and risk hazards associated with new payment systems.

With the number of attacks on the rise, it is clear that assigning more human resources is not a sustainable way to address the problem. Nor is it easy to find skilled cybersecurity employees. To add to the challenge, most security teams do not have the luxury of spending 100% of their time focused on security.

For many banking institutions, control can and should remain at the forefront of any security strategy for the organisation. The method to achieve that control requires a fresh approach that incorporates automation, integration and education.

**AUTOMATION** - Relying on manual processes to defend against modern and relentless attacks is inadequate. Attackers are taking advantage of automation and banks need to do so as well to reduce labour-intensive tasks and streamline processes. Tools that can intelligently identify and automatically issue alerts only on relevant security events can save security teams hours of investigating events that are not real threats and prioritise those that are the most relevant. In addition, being able to automatically provision, tune and enforce security policies and rules across control points without manual intervention efficiently minimises risk of exposure to the latest threats and vulnerabilities, despite dynamically changing environments in a banking organisation.

## Control can and should remain at the forefront of any security strategy for the organisation.

contain and stop damage and prevent future attacks. Plus the data gathered is usually a snapshot in time, and not continuously updated to monitor activity as it unfolds.

Instead, what is needed is a tightly-integrated banking security architecture that complements integrated visibility and analysis with integrated and automated controls enabled with central policy management, monitoring and distributed policy enforcement. Open Application Programming Interfaces (APIs) extend control capabilities to include existing and evolving security infrastructure.

**EDUCATION** - With automation and integration in place, highly-skilled security staff will be able to turn more of their attention to keeping up with the latest threats and techniques attackers use to disguise attacks, exfiltrate data and establish beachheads for future attacks. Ongoing professional development to remain updated on security best practices as well as how to optimise security technologies for maximum security effectiveness will help to ensure that banking organisations are getting the most from their IT security investments.

With a security approach that incorporates automation, integration and education, control is an achievable reality and a necessity to detect, understand and stop cyber risks especially those associated with new payment systems for banking institutions. \*

■ Ammar Hindi is Managing Director of Asia Pacific operations for Sourcefire, now a part of Cisco. He is responsible for corporate operations across the region, including sales, business development and strategic marketing activities.

# Aiming for zero downtime

DATA SECURITY IS A KEY CONCERN AS BANKS PURSUE MORE ONLINE TRANSACTIONS AND PAYMENTS. HOW CAN BANKS ACHIEVE ZERO DOWNTIME AND IMPLEMENT EFFECTIVE DISASTER RECOVERY PLANS TO PROTECT CUSTOMER DATA?

■ MULIA MOHAMED ONN

64

BANKING INSIGHT + JUNE 2014

**L**ast May, banks began reducing online banking fees per transaction from RM2.00 to RM0.10. At the same time, transaction fees for cheques were increased and are set to continue increasing in the next few years. Bank Negara Malaysia (BNM) cited the need for more effective and cost-efficient banking as the reason for the new pricing strategy.

## Explosion of Data

With the new targets set by BNM to increase electronic payments, one thing is sure: the amount of data a bank will need to host and protect is set to increase tremendously.

Online transactions have doubled since 2006 to 1.6 billion financial transactions in 2012. While BNM finds the progress positive, the target is to increase the number of electronic payments per capita from 56 in 2012 to 200 by 2020. BNM also intends to

reduce the number of cheques cleared in the country by half from 204 million to 100 million during the same period. If this is achieved, Malaysia will reap an annual savings of up to 1% of gross domestic product (GDP).

While the initiative by BNM is a win-win situation for both customers and banking institutions, the big question to ask is: how will banks ensure customer data will not be lost?

## Preparing for the Worst

One of the key guidelines BNM had issued ahead of these new changes was that financial service institutions (FSIs) must have good business continuity management and disaster recovery plans. Basically, FSIs need to have a backup plan and infrastructure implemented - in the event that their main data centre malfunctions due to a system failure, electrical outage or natural disasters such as fire, flood, tsunami or more, to ensure business continues as normal at all times.

Historically, malfunctions and disasters have occurred many times. These include power outages that caused vital online banking sites to go down, and website upgrades gone wrong where customers wake up to find their information has vanished. No matter how much infrastructure or capital banks have invested in their sole data centre infrastructure, technology can and will break down.

With only one data centre to host all their information, sensitive information like transaction history, account details and more could be lost; worse, the banks will not be able to recover the information. Imagine the nightmare of customers accessing their online bank accounts only to find a zero savings or current account balance!

With a secondary Disaster Recovery (DR) site in place, customers are assured that in the event of a main data centre collapse, business continues as usual as data can be accessed safely via a secondary data centre.

# Horror

Imagine the nightmare of customers accessing their online bank accounts only to find a zero savings or current account balance!

**IF A BANK IS UNPREPARED** to handle eventual disaster, why would a customer want to leave their money in that bank?

In this age of instant connectivity, any downtime reflects badly on a business' reputation. When a customer is unable to access their banking account or worse, sees missing financial records, it causes uncertainty. They will want to instantly move their money to another bank.

Otherwise banks will have to face unhappy customers each time their website is down or services are inaccessible. The worst case scenario would be missing money.

Where is data stored? Is there a secondary site? Are both sites managed reliably? These will probably be among the questions banks will frequently have to answer in the near future as customers become more aware about data and the security of their online transactions.

If BNM is to achieve its target for online transactions, banks need to work hand-in-hand and place utmost priority on ensuring their business continuity plan is in place and supported with a well-managed secondary DR site.





## What to Look out for When Planning Data Centres

Connectivity, infrastructure, technical support and compliance are some of the factors banks need to look at before deciding on a data centre. Most importantly, the data centre needs to be well-equipped and monitored 24/7. Place emphasis on how often health checks are done on the centre's infrastructure, the strength of the technical team and so on and so forth.

Regular network infrastructure, system and application health checks must be done to ensure data remains safe and accessible. The data centre must also have independent auditors that come in to perform penetration tests (pen tests) on the network and systems.

These data centres must also be properly certified with certifications such as ISMS, ITSM and PCI DDS.

- ISMS (Information Security Management System) emphasises that an organisation should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.
- IT Service Management (ITSM) is a process-based practice intended to align the delivery of information technology (IT) services with the needs of the enterprise, emphasising benefits to customers.
- Compliance with the Payment Card Industry Data Security Standard (PCI DSS) means that their systems are secure, and customers can trust banks with their sensitive payment card information.

Technology regularly breaks down. Even with all the necessary health checks in place, it can malfunction. The only difference is that banks have a higher chance of predicting a malfunction when the system and infrastructure is well maintained.

Similarly, bank services can face downtime if the banks' telecommunications carrier is down. This is why data-intensive organisations like banks must ensure that they have more than one choice of carrier or provider to fall back on in the event of a downtime. A data centre that limits banks to one carrier is a risky choice as banks lack the flexibility of choosing the right partner to match their business needs.

With a carrier-neutral data centre, banks can choose to have one or more telecommunication providers. This is important when implementing a business continuity plan as in the event of a network failure or fibre cut, the bank will have another carrier to support its business. In addition, options give banks the flexibility to pick the

connection package that best suits their business needs.

**A data centre that limits banks to one carrier is a risky choice as banks lack the flexibility of choosing the right partner to match their business needs.**

Furthermore, in the event that banks decide to switch their telecommunication partner, all they have to do is switch over without having to physically move any of their infrastructure to another data centre, saving them time and cost. Carrier-neutrality also gives banks the added advantage of competitive telco rates to choose from.

Banks also need to look at the power resource capabilities of a data centre as data centres need to operate 24 hours a day and must be constantly powered. Find out if there is a back-up energy source and how the power is being managed as data centres consume a high amount of energy. Through proper best practices, they should be able to minimise heat with proper cooling systems in place to ensure power consumption is maintained. This is important as at the end of the day, power consumption makes up a sizeable fraction of the cost of hosting data. When making a choice take into account the new market trends, review security and privacy standards and so forth.

Policymakers need to constantly review the security and privacy standards based on market trends, consumer appetites and geological conditions. The world is moving at a fast pace and data is growing at breakneck speed. Banks need to constantly evolve with the times to ensure they remain up-to-date with the business requirements of enterprises. Data is a serious business and when it involves money, it is essential that the best, most flexible and reliable service providers are put on the job. \*

■ Mulia Mohamed Onn is Vice-President, Enterprise Sales of AIMS Group, a leading carrier-neutral data centre operator and managed services provider in Malaysia and Southeast Asia. Located in the central business districts of Kuala Lumpur and Cyberjaya in Malaysia, AIMS provides international class data storage facilities and ancillary services, augmented by an unrivalled platform for interconnectivity, making it one of the most interconnected sites in Malaysia and Southeast Asia.



# ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM (AML/CFT)

A relevant qualification that enhances your capability.

Understanding the complexities surrounding this important aspect of banking is definitely an asset. IBBM's Professional Qualifications and Training in Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) are designed to improve your financial institution's operations and compliance as well as add value to your profession.

**Our next intake is August 2014, so visit us at [www.ibbm.org.my](http://www.ibbm.org.my) and sign up today.**

Jointly Awarded by:



Institut Bank-Bank Malaysia  
Institute of Bankers Malaysia



International Compliance Association  
Excellence through Education



The University of Manchester  
Manchester Business School

Supported by:



AIF  
ASIAN INSTITUTE OF FINANCE

Phone: 03-2095 8922 | Fax: 03-2095 2322 | Email: [marketing@ibbm.org.my](mailto:marketing@ibbm.org.my)

 [www.ibbm.org.my](http://www.ibbm.org.my)

 [www.facebook.com/IBBMalaysia](http://www.facebook.com/IBBMalaysia)

 [@IBBMalaysia](https://twitter.com/IBBMalaysia)

 Institute of Bankers Malaysia

# GRACE 2014



---

**17<sup>th</sup> IBBM Graduation and Awards  
Ceremony  
Majestic Hotel, Kuala Lumpur  
31 May 2014**

For more information,  
visit [www.ibbm.org.my](http://www.ibbm.org.my) or  
email [grace2014@ibbm.org.my](mailto:grace2014@ibbm.org.my)