Exclusive Interview with AICB Chief Executive Edward Ling
'To Walk Far, We Walk Together'

BANKING INSIGHT

IDEAS FOR LEADERS | **DECEMBER 2022**
PP 17327/05/2013(032407)

Will the Adults in the Room Please Stand Up

Battling climate finance myopia means that we have to be present at the table.

The Strategic Value of Threat Intelligence

FINANCIAL CRIME ON THE NEW FRONTIER: SCAMS ASSOCIATED WITH CRYPTOCURRENCY

A PUBLICATION OF
AICB
ASIAN INSTITUTE OF CHARTERED BANKERS
ISSN 2231-6247

FAKE NEWS: CAN YOU HANDLE IT?


MYCO ID: 201201039737
Frankfurt School of Finance & Management
German Excellence. Global Relevance.
ASIAN BANKING SCHOOL
Equiping senior management from banks and other financial-related organisations with the know-how to lead institutions into a more sustainable (business) world. Taught by renowned faculty and leading industry experts from one of the top business schools in the world.
ABS | Executive Education
LEADING THE SUSTAINABILITY TRANSFORMATION IN BANKING
2ND EDITION · 8 - 12 MAY 2023 · FRANKFURT, GERMANY
This is a HRD Corp claimable programme. Employers can claim up to 100% of the course fee, airfare, accommodation and daily allowance.
For more information on the programme, visit: www.asianbankingschool.com
To register your interest, email: training@asianbankingschool.com / call: +603-2742 7822
HRD CORP CLAIMABLE
AICB 40 CPD HOURS

Editor's Note

In the Zone

When flying an aircraft, the most difficult manoeuvre is a short-field landing. That is when the landing strip is shorter than usual and the pilot's true ability is put to the test. If you flare too fast, the aircraft drops abruptly; too slow, then you land hard or flat; misjudge the distance and you run out of runway.

But when you get it just right, even the toughest landing feels like auto cruise. That's when you know you're in the zone.

In many ways, this experience mirrors that of the modern banker – where every day is a short-field landing. While we can't change the realities of this industry, we can change our approach to its stressors, and if we get the formula right today, there's a good chance the future finds its own soft landing.

This is the impetus behind the AICB's inaugural Malaysian Banking Conference 2022, with its special focus on environmental, social, and governance (ESG) issues and our 500-strong delegation tackled the tough questions in order to steer the banking sector and nation forward in its ESG goals. Finance, with its potential to set the sustainability agenda by directing capital towards net-zero aspirations, is a critical component in realising a greener and better future for all. Given its important contributions to environmental sustainability and financial inclusion – through the Joint Committee on Climate Change, the ASEAN Green Taxonomy, and more – Malaysia is assured of its seat at the table, however, it also means we have a greater duty of care.

I also reflect on this year's International Conference on Financial Crime and Terrorism Financing and my personal, intense discussions with members on what keeps them up at night. It reminds me of the clarion call by Tan Sri Nor Shamsiah Mohd Yunus, Governor of Bank Negara Malaysia, whose keynote address called for vigilance in the ever-expanding borders of crime: "We are now at a new frontier of compliance. The fight against financial crimes is one fought on multiple fronts and the chain is only as strong as the weakest link."

"Our success requires all parties; the private sector, regulators, law enforcement agencies and other government bodies, and consumers alike, to do their part – **TO ADAPT TO THESE NEW THREATS, TO TRANSFORM THEMSELVES TO DEAL WITH THESE CHALLENGES,** and to collaborate to safeguard the integrity of our country's financial system."

"Our success requires all parties; the private sector, regulators, law enforcement agencies and other government bodies, and consumers alike, to do their part – to adapt to these new threats, to transform themselves to deal with these challenges, and to collaborate to safeguard the integrity of our country's financial system."

The flagship publication of the AICB, *Banking Insight*, is a key resource for our members. In this December 2022 collection, our feature articles reflect matters that are at the forefront of an increasingly complex and interconnected world. From 'soft' issues such as honouring moral codes and Empathetic Banking to regulatory guidance on artificial intelligence and quantum hacking, the subjects are as diverse as the skills needed to navigate the terrain.

As a lifelong aviation enthusiast, mastering the touchdown is constant work in progress – and I believe the professionalisation of banking demands the same. For 2023, let's resolve to get in the zone, and get more things right. ✱

The Editor

PUBLISHER
Asian Institute of Chartered Bankers
197701004872 (35880-P)
(formerly known as
Institut Bank-Bank Malaysia)
Levels 11 & 12, Bangunan AICB
10 Jalan Dato' Onn
50480 Kuala Lumpur, Malaysia
Tel +603 2602 6833 / 1300 88 6833
Email enquiries@aicb.org.my

PUBLISHING CONSULTANT
Executive Mode Sdn Bhd (317453-P)
Tel +603 7118 3200
Fax +603 7118 3220
Email info@executivemode.com.my

PRINTER
Empress Print Sdn Bhd
No. 33, Jalan PBS 14/8
Taman Bukit Serdang, Seksyen 14
43300 Seri Kembangan
Selangor Darul Ehsan
Tel +603 8959 9233

CONTENTS | DECEMBER 2022

Pathway to Net Zero

Chairman of AICB, Tan Sri Azman Hashim, FCB (fifth from right); together with the AICB Council; Chief Executive Edward Ling (far right); and YB Tengku Zafrul, FCB (seventh from left).

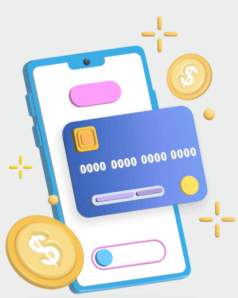
The inaugural Malaysian Banking Conference, held from 12–13 September 2022 in Kuala Lumpur, was jointly hosted by the AICB and The Association of Banks in Malaysia. The highly charged event convened over 30 leading sustainability experts and 500 delegates on the theme of 'Banking on Change: Turning the ESG Momentum into Action'.

Zeroing in on tangible climate action, the discussions traversed the ruddy but promising landscape of climate change and the critical role of the Malaysian financial sector in what the UN has called the Decade of Action. Robust discussions ensued, including defining Malaysia's environmental, social, and governance (ESG) promises, transitioning to a low-carbon economy, climate data and disclosures, workforce transformation, and navigating the ever-evolving risks of the ESG landscape.

With a special address by the then Minister of Finance YB Senator Tengku Datuk Seri Utama Zafrul Tengku Abdul Aziz, FCB, the engaged format featured in-person panel discussions, plenary sessions, diverse breakouts, a half-day masterclass, and a Chartered Banker Roundtable facilitated by Dr Ben Caldecott, Founder and Director of the Oxford Sustainable Finance Group, University of Oxford.

SNAPSHOT – GLOBAL FINANCIAL INCLUSION

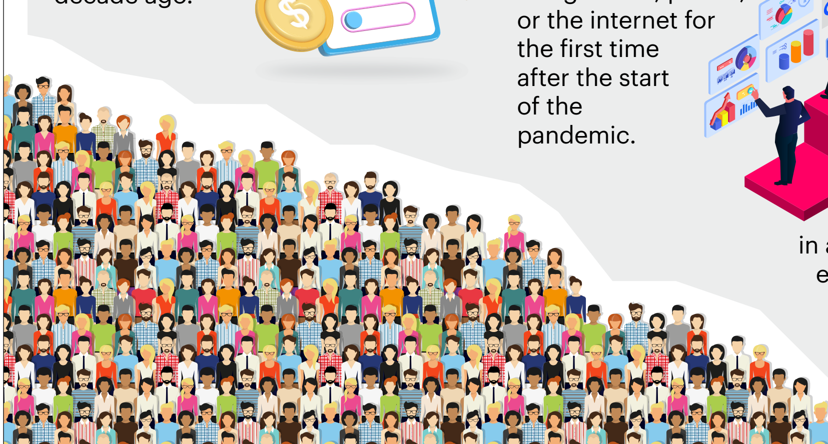
76% of the global population have a bank account, up from 50% a decade ago.



40% of adults in developing economies, excluding China, made a digital merchant payment using a card, phone, or the internet for the first time after the start of the pandemic.

Only **55%** of adults in developing economies can access extra funds within 30 days if faced with an unexpected expense.

SIX percentage points is where the gender gap in account ownership across developing economies stands, a marked reduction from nine percentage points where it hovered for many years.



SOURCE: *World Bank, Global Findex Database 2021.*

SHARPENED FOCUS ON FINANCIAL CRIME

Global financial crime experts and banking industry specialists gathered in Kuala Lumpur for the 12th International Conference on Financial Crime and Terrorism Financing (IFCTF) from 26–27 July 2022. Jointly organised by the AICB and Compliance Officers' Networking Group, this industry feature event was supported by Bank Negara Malaysia, Securities Commission Malaysia and the Labuan Financial Services Authority and convened over 900 industry delegates with 50 global experts focused on intensifying the fight against white-collar crimes.

Themed 'The New Frontier of Compliance: Adapt, Transform, Collaborate', AICB Chairman, Tan Sri Azman Hashim, FCB, emphasised in his welcome address the objective of the Chartered Banker qualification in the collaborative financial network that has been built by AICB: "We continuously work closely with industry and relevant partners to build and strengthen the competence and skill sets of the financial sector workforce in compliance and AML/CFT through the various certifications that we offer. We hope these efforts will contribute strongly to building a sustainable local pipeline of finance practitioners equipped with the capacity and capabilities to combat the scourge of financial crime, and preserve the sanctity of the financial system upon which millions of people depend."

From left: Faradina Ghouse, CB, Chairman of AICB's Compliance Officers' Networking Group; Tan Sri Azman Hashim, FCB, Chairman of AICB; Tan Sri Nor Shamsiah Mohd Yunus, Governor of Bank Negara Malaysia; Datuk Seri Mustafar Ali, Director-General of the National Anti-Financial Crime Centre; Dato' Khairussaleh Ramli, FCB, Vice Chairman of AICB.

QUANTIFYING METRICS FOR OPERATIONAL RESILIENCE

The Basel Committee on Banking Supervision (BCBS) tees up on operational resilience through consultations with jurisdictions on a guiding set of principles to ensure essential services are uninterrupted in the face of pandemics, large-scale system outages, or natural disasters.

Although banking has proven to be resilient during this crisis, the concern is whether the system can withstand shocks that are large enough to trigger significant second-order financial consequences and loss of confidence. An independent 2021 study commissioned by the European Central Bank highlighted an operational failure of the TARGET2-Securities system, a centralised platform for the settlement of securities transactions within the European Union, in May 2020, which caused a halt of over 740,000 transactions for approximately 12 hours, resulting in a daily disruption value in excess of EUR1 trillion.

The BCBS' broad principles on operational resilience are not prescriptive, and acknowledge that each jurisdiction will take differing approaches and set its own benchmarks for return to operational functionality following an outage.

On this score, some jurisdictions have already started the ball rolling. For instance, the US Financial Stability Board's (FSB) white paper, *An Approach to Quantifying Operational Resilience Concepts,* issued on 1 July 2022, explores 'output-based resilience', a quantifiable measure of systemic resilience by determining what the base level of 'critical functionality' is for a complex system, measuring the degree to which a disruption reduces that critical functionality, and how quickly the system recovers from that reduction.

The FSB paper also explores assigning a dollar value to measure the cost of disruption (defined as an interruption in the ability to deliver functionality as a result of the manifestation of some operational risk, such as a natural disaster or cyberattack) based on the size and resilience required at each level of event security.

Banks should cast a keen eye on developments in this rapidly growing topic in regulatory circles as quantifying resilience informs all aspects of critical operations, including risk mitigation and tolerance-setting thresholds.

CRYPTO 'BANK RUN' SPARKS CHAIN OF PAIN

In May 2022, the popular cryptocurrency TerraUSD (UST) crashed due to sell-offs from unknown sources. The uncollateralised stablecoin was designed to be pegged against the US dollar and maintained its set price by pegging itself against another sister currency, Luna tokens. When news circulated that one of Terra's main developers and another unknown user had sold off 234 million UST, other UST depositors began withdrawing the stablecoin, which knocked UST off its USD1 peg. This spiralled into the virtual-world equivalent of a bank run for the stablecoin, with panic selling of UST and Luna token said to have cost investors USD60 billion in real cash.

The flood of UST and Luna token transactions created a domino effect for cryptocurrency-focused hedge funds that had been lured by the high payoffs touted by UST, and retail holders who had been promised as much as 20% annual returns.

One of the biggest casualties was Three Arrows Capital (3AC), a Singapore-based cryptocurrency-focused hedge fund that had invested between USD200 to USD560 million in Luna tokens that were rendered worthless in a matter of days.

Founders of the USD10 billion hedge fund went on the lam after authorities in several jurisdictions – British Virgin Islands, the US, Singapore – ordered 3AC's liquidation in June and commenced criminal investigations.

Ironically, among the laundry list of creditors is 3AC co-founder Su Zhu, who filed a USD5 million claim from his own hedge fund and was rumoured to have bought a USD50 million yacht with investors' money before the house of cards came tumbling down.

The Monetary Authority of Singapore has stated that 3AC was found to have provided false information as it had exceeded the SGD250 million threshold that a registered fund management was permitted to oversee. Investigations are ongoing at the time of writing.

Poor risk management or criminal cyber mastermind? You decide.

Wanna Talk About It?

There is an inextricable link between human well-being and economic health. For instance, in terms of per capita gross domestic product (GDP), the world's citizens are better off today than they were a decade ago, but do they feel safer, less anxious, more optimistic about the future?

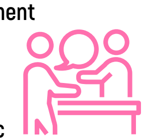
"Just as good health — mental and physical — is fundamental to individual well-being, public health is fundamental to stable, cohesive societies. That is the lesson we must take from the Covid-19 pandemic," writes Gita Bhatt, Editor-in-Chief of the International Monetary Fund's monthly magazine, *Finance & Development*, which advocates for global adoption of a personal well-being index to measure national well-being, in addition to metrics such as GDP.

Meanwhile, McKinsey & Co proposes three key actions companies in Asia should undertake to create a flourishing, positive work culture in its August 2022 article, *Employee Mental Health and Burnout in Asia: A Time to Act:*

Effectively addressing toxic behaviours: Take the courageous and uncomfortable step of taking an honest look for toxic workplace behaviour.

Right resources to serve employee needs: Combine foundation-level and tailored support for your people.

Improved measurement and organisational listening capabilities: Increase measurement quality and take holistic action.



'To Walk Far, We Walk Together'

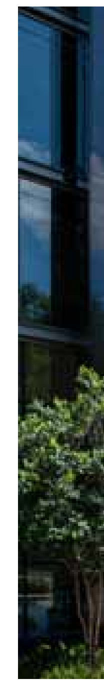
By Dr Amanda Salter

In an exclusive interview with ***BANKING INSIGHT*, CEO EDWARD LING** discusses what it means to be at the helm in a post-Covid world.

My first impression of Edward was of a serious man, some might even call him 'guarded'. As we continued to speak however, he quickly opened up to reveal another side to his demeanour – insightful, intelligent, determined, with a keen sense of humour.

Edward's people-centred ethos stood out strongly to me, a collaborative leadership style with a focus on long-term impact. He is a man who clearly relishes new challenges and hungers for continuous learning.

This article summarises the highlights from our conversation, including his first year on the job, his leadership style, what the Institute brings to the global stage, as well as the course he is charting for the next few years.



Q ***Edward, you've steered AICB through one of its most significant years so far. What does it mean to you personally, to lead this Institute during one of the most tumultuous times in recent history?***

Many people equate the CEO position with power. I prefer to emphasise the responsibilities that come with the job because with much power comes much responsibility; my job is to steward that power and authority responsibly.

One of my first missions since coming onboard in September 2021 has been to listen and to understand the expectations of our stakeholders, which include the membership, Council members, my team and our partners. There is no doubt in my mind that the organisation and members' best interests must come first, even ahead of my own.

This is necessary in understanding and positioning the Institute so that people realise the value proposition of AICB, what we bring to the table because we occupy a unique space in the financial services sector. There is an ultimate goal in mind – something that would mark that we've arrived to the next level of maturity as an organisation – and we're working tirelessly to get there. But no matter how much we plan for things to be predictable and controllable, they rarely are. We need to anticipate what's coming down the track to meet us, and plan how we will tackle the challenges that are on the horizon.

The next step was to bring my team with me on this journey to chart the Institute's next phase of growth. I am a firm believer of the adage, "if you want to walk fast, walk alone; but if you want to walk far, walk together". Coming up with a plan is not actually difficult, what's crucial is that we get everyone travelling in the same direction, to ensure that everyone understands and adopts the same vision. "How do I bring people with me?" is very important,

One of my first missions since coming onboard in September 2021 has been to **LISTEN AND TO UNDERSTAND THE EXPECTATIONS OF OUR STAKEHOLDERS, WHICH INCLUDE THE MEMBERSHIP, COUNCIL MEMBERS, MY TEAM AND OUR PARTNERS.** There is no doubt in my mind that the organisation and members' best interests must come first, even ahead of my own.

otherwise it will be a very lonely journey, and I don't think we'd last very long. We need a team mindset.

Q ***What keeps you on track in this journey – what's your North Star?***

We need to rally around one single purpose – how and why we exist.

The AICB is a professional qualification institute, and that makes us a membership body, albeit a niche one. We exist because of the qualifications we offer, the standards we uphold, and the elevation which the Chartered Banker status confers. These aspects make us not just a membership body, but one that represents the best of banking.

In this way, it's very important that we stay true to our core purpose, the reason we exist. Our members' opinions matter; they have a crucial say in what their vision for AICB is. Coupled with the lateral vision of our Council, who are captains of industry, the Institute gains its gravitas. This shared understanding is key and must be the starting point in everything we do. How we get there is my responsibility.

I believe we've got much of the formula right. Our 2021 membership survey puts us in good stead: 94% agree that our professional qualifications equip them with the requisite skills to succeed in banking today; 83% believe that being an AICB member has contributed to their career growth; and 92% are proud to be associated with the brand and would retain their membership, even on a voluntary basis.

Q ***What are your plans for AICB over the next few years?***

How do I explain this without divulging company secrets? *[laughs]*

Here's what I believe: it's easy to grow membership numbers, but retaining and creating an engaged, beneficial community is a tougher goal to achieve. Which is why my team and I are focused on these four key areas for the Institute:

Retention – we want to retain our members and grow with them. If you're a good membership organisation, people will stay with you forever; if you're not so good, they join, they lose interest and leave. We want AICB members to enjoy being a part of this organisation, to enjoy the values and benefits that we provide; not just today, but throughout their professional careers and beyond. Digitalisation is a big part of the projects we're undertaking to get members onboard with remote access learning, to move the dial up from 60% who currently use our online platform for continuous learning. Our other curated events, such as this year's inaugural Malaysian Banking Conference, jointly organised with The Association of Banks in Malaysia, and the annual International Conference on Financial Crime and Terrorism Financing, are avenues that go beyond competency building – they foster collaboration and a sense of belonging among industry members.

Reputation – trust isn't easy to build.

Digitalisation is a big part of the projects we're undertaking to get members onboard with **REMOTE ACCESS LEARNING, TO MOVE THE DIAL UP FROM 60% WHO CURRENTLY USE OUR ONLINE PLATFORM** for continuous learning.

It's important that others perceive AICB to be the embodiment of the values we expect of the industry. Our standing as a premier professional body depends on the continued positive perception of the expertise, qualifications, networks, and services that we provide. It also comes through in our actions and the value that we deliver to members.

Rigour – maintaining the standard of our qualifications is key. Without such rigour, our membership growth would accelerate, but it would not be sustainable. Unlike broad-based membership organisations, the Chartered Banker designation – jointly conferred in this region by the Chartered Banker Institute (CBI) UK and the AICB – has a bigger purpose. It is a route to rebuilding public confidence and trust in banking and bankers since the global financial crisis.

Relevance – our content and how it is delivered must reflect today's conversations and tomorrow's concerns. The Institute must be the first port of call for our members, not just on ongoing issues in the mainstream like regulation and financial resilience, but on discussions that are unfolding at the fringes of banking, issues that are not yet knocking at our doorstep but will be very soon. Partnerships, in this respect, are key. We cannot possibly know all there is to know in finance, and this is where we leverage the knowledge and specialisms of our global partners and institutional networks, by giving them in-person and remote access to engage with top experts in the field.

Q ***You mention that partnerships are key. What partnerships are you investing in at AICB?***

We are privileged to have the very best in the industry with us.

The CBI in the UK, with whom our Chartered Banker qualification is jointly awarded, sets the bar, not just in devising banking qualifications and assessments, but also through their know-how and preparedness in times of uncertainty. For instance, throughout the pandemic, we worked shoulder to shoulder in migrating all our exams from physical sessions to online within two months with zero interruption or service failure – a huge achievement.

We also partner with the Bangor Business School, UK, one of the world's top 10 schools in banking, to award the Chartered Banker MBA. This programme gives our members an accelerated pathway to gain both the Chartered Banker status and an MBA at the same time.

Our sister organisation, the Asian Banking School, whose campus is a stone's throw away from the Institute, works with us to deliver world-class training workshops. In this way, we leverage their sector-leading executive education programmes with some of the top business schools in the world, including the Cambridge Judge Business School at the University of Cambridge, to raise the competency standards for our membership.

These collaborations allow us to

Our standing as a premier professional body depends on the **CONTINUED POSITIVE PERCEPTION OF THE EXPERTISE, QUALIFICATIONS, NETWORKS, AND SERVICES** that we provide. It also comes through in our actions and the value that we deliver to members.

innovate our qualification pathways. For instance, in addition to our Chartered Banker pathway, we've also mapped out an experiential pathway for our members via the Chartered Banker By Experience programme, to reflect the rich and diverse talent pool of senior leaders in industry. We recognise that experience holds its own value and AICB is a great platform to connect the generations of banking professionals, so that they learn from each other too in informal ways.

Q *Earlier we touched upon innovation. What you said echoes some of what I've experienced in the digital consulting sphere, that well-established organisations are often edged out of relevance and we've got to be cautious about that.*

It's true. Established organisations tend to do the same thing over and over, thinking that they're at the top of their game and continue to work what they feel to be a winning formula. Once this mindset creeps in, that's when the organisation begins slowing down – they stop innovating, they're less quick to try out new things, and they underestimate the competition.

AICB is more niche and this focus makes us agile enough to innovate at the pace of today's changing business environment. We do share some common risks and challenges with other established professional bodies and quite often the strategies can seem similar to an outsider who is looking in. But the inner workings of each organisation can be worlds apart.

We shouldn't be afraid of things that we're not familiar with, especially with the new generation entering the talent pipeline – the way they learn and want to learn things is different. We must be modern, different, and fresh; we must meet expectations head on.

Q *My final question: I've heard that you're a fan of the Civilization* video game. What part of it fascinates you?*

[laughs] It's one of my guilty pleasures, although I haven't gotten around to it lately.

I've always enjoyed strategy and tactical pursuits, even on my days off, and I've been a fan of this game ever since it first came out in 1991. Building a virtual empire isn't just about defence and attack, and dominance isn't achieved solely by invading other empires – you can also win through science and technology, or through culture.

It requires me to think hard about how to manage my civilisation. There are so many things you need to juggle, so many interests to consider. It was probably one of the best leadership training tools in those early years of my career that still resonates with me today.

Just like Civilization, there are many types of leaders in this world. You pick and choose your leadership style, and your ethos shapes how you play the game. Some leaders focus purely on making money, without thinking much about the environment, social factors, or governance (ESG). But others take a broader view, they want to do well in terms of ESG and embed it as part of their definition of success – my money is on these organisations. They're the ones who will actually enjoy lasting success.

**The award-winning strategy game by Sid Meier in which players battle to build empires that will stand the test of time.* ✱

■ *Dr Amanda Salter is Associate Director at Akasaa, a boutique content development and consulting firm. She has delivered award-winning customer experience strategies for the Fortune 500 and been an Agile practitioner for over a decade. Previously with Accenture's London office, Dr Salter holds a PhD in Human Centred Web Design; BSc (Hons) Computing Science, First Class; and is a certified member of the UK Market Research Society and Association for Qualitative Research.*

WILL THE ADULTS IN THE ROOM PLEASE STAND UP

By Angela SP Yap

Battling climate finance myopia means that we have to be present at the table.

On 28 October 2022, one of the biggest global finance-led climate-change initiatives, the Glasgow Financial Alliance for Net Zero (GFANZ), made headlines as it has quit the United Nations' (UN) Race to Zero (RtZ) campaign. In 2021, GFANZ made it a rule that all members "must align with the RtZ criteria". In less than a year, cracks had formed and its latest 2022 report reads that GFANZ will instead "continue to engage regularly" with RtZ and other global climate groups with a note that any guidance issued is voluntary.

Led by former Bank of England Governor Mark Carney and backed by billionaire Michael Bloomberg, GFANZ was launched during the UN's 26th Conference of the Parties (COP26) Summit in April 2021. At the time, GFANZ membership comprised of 160 of the world's biggest banks and pension funds who cumulatively controlled over USD70 trillion worth of assets (currently it has over 400 members with over USD130 trillion in assets). RtZ is the net-zero standard-setting body tasked with overseeing compliance of member organisations, including GFANZ.

The alliance was historic as members of the finance coalition pledged to responsibly steward financial flows in order to accelerate the transition to net zero by 2050. This meant that the world's biggest banks would commit themselves to transformative lending patterns and practices to nudge economies on the path to limit global warming to 1.5°C. Even then, climate experts and campaigners were sceptical.

At the time, GFANZ membership comprised of 160 of the **WORLD'S BIGGEST BANKS AND PENSION FUNDS WHO CUMULATIVELY CONTROLLED OVER USD70 TRILLION WORTH OF ASSETS** (currently it has over 400 members with over USD130 trillion in assets). RtZ is the net-zero standard-setting body tasked with overseeing compliance of member organisations, including GFANZ.

FALLOUT

The latest criteria issued by RtZ, in June 2022, raises the bar and requires member organisations to phase out the future development, financing, and facilitation of fossil fuel assets, such as coal, and publish transition plans for Scope 3 emissions (indirect greenhouse gas emissions generated as a result of activities undertaken either upstream or downstream). RtZ also warns that members should not be exposed as "trying to find loopholes" to the new guidelines which come into effect from June 2023 onwards.

In response, Australia's superannuation fund, Cbus, and Austria's *Bundespensionskasse* pension fund, withdrew from the Carney-Bloomberg green alliance, stating that the data tracking and reporting requirements under RtZ compliance were too complex and excessively resource-intensive. Other global systemically important banks, including JP Morgan, Morgan Stanley, and Bank of America, said that they would leave the alliance as RtZ policies put them at risk of lawsuits and may be at odds under the existing and upcoming Securities and Exchange Commission rules. Speaking under condition of anonymity, *The Globe and Mail* quoted a source who said a bloc of Canadian banks also had concerns over the legal implications of RtZ's requirement to withdraw financing from the fossil fuel industry. Even supervisory authorities have expressed concerns, with the European Central Bank noting that RtZ and similar criteria will put GFANZ member banks at risk of lawsuits if they fail to deliver on their pledges.

There is a limit to the credibility of 'voluntary initiatives that leave it to their voluntary members to volunteer what to do' no matter how many volunteers they have managed to bring 'into the tent' with extremely lenient entry requirements. Today's announcement that GFANZ will go it alone, a week before COP27, leaves its credibility hopelessly shattered. It is high time for **GOVERNMENTS TO FINALLY STEP IN AND REGULATE THE FINANCIAL INDUSTRY TO COMPLY WITH THE PARIS CLIMATE GOALS.**

As impact investing and environmental, social, and governance (ESG) concerns gain ground in the international financial sector, it seems inevitable that the chasm will widen between the non-profit sector and financial services on what it takes to go green.

According to sources who spoke to *FT* this September, the heavyweight banks in GFANZ felt blindsided by the tougher UN climate criteria and that its legal implications had not been considered in advance by the standard-setting body.

"I am close to taking us out of these global green commitments — I'm not going to allow third parties to create legal liabilities for us and our shareholders. It is immoral and irresponsible," said one senior executive at a US bank during internal discussions. "What if we get it wrong, make a mistake or someone lies? Then the bank can be sued, that is an unacceptable risk." The hour-long discussion also raised how newly proposed SEC rules "could add hundreds of pages to annual reports and require a small army of extra accountants and lawyers to produce and vet the data, which…is not yet reliable or properly codified."

Meanwhile, civil society organisations (CSOs) and climate activists are chiming 'I told you so'. Voices such as Johan Frijns, Executive Director of BankTrack, who said: "'GFANZ cutting ties with the UN-backed Race to Zero campaign is yet another example of how financial institutions always seem more keen on appearing to act on climate change rather than actually doing so. There is a limit to the credibility of 'voluntary initiatives that leave it to their voluntary members to volunteer what to do' no matter how many volunteers they have managed to bring 'into the tent' with extremely lenient entry requirements. Today's announcement that GFANZ will go it alone, a week before COP27, leaves its credibility hopelessly shattered. It is

high time for governments to finally step in and regulate the financial industry to comply with the Paris climate goals."

Such behaviour begs the question, are there adults in the room?

BECAUSE I TOLD YOU SO

BankTrack's comment that such behaviour is par for the course in banking and bankers is, in this author's opinion, either naïve or disingenuous. Even in climate policy circles, leading minds such as Dr Peter J May, Distinguished Professor Emeritus of American Politics at the University of Washington opine that "[t]he notion that regulations should be based on achievement of specified results rather than on adherence to particular technologies or prescribed means has been widely accepted as a basis for improving social and environmental regulations. The concept of performance-based regulation has been endorsed by the Bush and Clinton administrations, by a variety of business and environmental groups providing consensus proposals for reform of environmental regulations, and by various groups recommending regulatory reforms in other areas of regulation."

What CSOs like BankTrack are backing is a prescriptive regulatory regime, a rules-based system where requirements are granular and explicit, right down to minute system settings and reference codes. Research has found that over-regulation not only reduces the possibilities for innovation; it drives more opportunistic behaviour such as regulatory arbitrage, shadow banking, and other opaque market behaviour. It is also the reason why supervisory authorities have in recent times been applying a more goals-based approach in growing sectors such as fintech, cryptocurrency, and climate investing.

Research by Dr Christopher Decker at the University of Oxford, presented in the paper *Goals-based and Rules-based Approaches to Regulation,* cautions for why it is important to get the right regulatory mix:

"A rules-based approach generally involves rules that are precisely drafted, highly particularistic, and prescriptive; gives regulatees advance notice as to what actions they can and cannot engage in; and provides no or limited exceptions, and limited flexibility in any specific factual context. In contrast, a goals-based approach typically involves the setting of goals, outcomes, principles or standards, usually cast at a high level; a lack of prescription about how regulatees achieve these requirements; and requires regulatees to exercise judgment to predict what actions will achieve the regulatory objective.

"In practice, the choice of approach – goals-based regulation (GBR) or rules-based regulation (RBR) – in specific contexts can have significant consequential effects. Various assessments have associated the adoption of the RBR-type approach in a particular area with the poor performance, or even failure, of the relevant regulatory system. However, the adoption of a GBR-type approach in some areas has also been associated with regulatory problems."

The evidence, per Dr Decker, is that "the balance of advantages to disadvantages of each approach (GBR or RBR) depends on the context in which it is applied". Such contextual considerations include:

+ the timing of intervention and costs of each approach;
+ simplicity or complexity of the context;
+ nature of the risks regulated and potential for regulatory error;
+ information conditions;
+ degree of innovation;
+ the attitude and capabilities of regulatees;
+ communication, shared understandings, and predictability;
+ ability of regulator to adapt to an alternative approach;
+ ability to craft rules to capture the actions or activities of interest;
+ identifying and evaluating goals and outcomes; and
+ incentives to comply and the risk profile of regulatees.

The operative words being 'balance' and 'context' – both of which seem to have gone over the heads of many throughout the GFANZ-RtZ debacle.

STUCK WITH THE BILL

You can't insist on ordering everything on the menu, then stick someone else with the bill. That's just bad manners. However, that is what RtZ did.

Its imposition and short phase-in period of climate standards for banks are out of step with the realities of lending – the interconnectedness of structured products, minutiae of legal agreements, system architectures, and accounting rules. Their proposed rules would likely cause a systemic default that would rupture financial stability.

As far back as September 2021, the Bank of International Settlements (BIS) warned of a build-up of green asset bubbles as the global ESG push drives up the price of eco-friendly investments. The European Securities and Markets Authority echoed the same earlier this year, adding that geopolitical tensions and inflation caused lingering concerns about green asset overvaluation and "investors should consider the risk of market corrections".

Recent numbers also show a dip in ESG flows since global economies began reopening. The UK's largest investment platform, Hargreaves Lansdown, said that these funds were 115% lower year-on-year this January and others such as Aviva Investors' Chief Executive, Mark Versey, told *FT* that some green stocks are "frankly overpriced" and that "buying brown and helping it to become green will deliver better investment returns, and it doesn't matter what asset class you're talking about".

GREEN IS NOT RISK-FREE

Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, said it best in his speech, *A Resilient Transition to Net Zero,* at the Conference of Montreal last July:

"The primary role of prudential regulation is to mitigate risks to banks. A resilient and healthy banking system is one that can best support households and businesses through the provision of key financial services, also during the transition to net zero. As such, prudential regulation forms part of a much broader set of tools and measures – including fiscal, technological, or legislative – when it comes to responding to climate change and the transition to net zero.

"We already have a goal and instrument when it comes to the resilience of banks, and should therefore refrain from using prudential regulation to meet other climate-related objectives (such as promoting 'green-type' investments). We should be setting capital requirements based on the inherent risk profile of each asset class.

"In transitioning towards net zero, the risks to banks are two-sided. While much of the focus has rightly been on exposures to 'brown' assets that risk becoming stranded over time, we should also remain vigilant to the risks from 'green bubbles'."

The primary role of prudential regulation is to mitigate risks to banks. **A RESILIENT AND HEALTHY BANKING SYSTEM IS ONE THAT CAN BEST SUPPORT HOUSEHOLDS AND BUSINESSES** through the provision of key financial services, also during the transition to net zero.

REMEMBERING THE TSUNAMI

Perhaps what will work is to reframe the narrative for banks – that climate change is not another cost to absorb, but a key factor in banks' crisis preparedness measures.

After all, a climate-induced financial crisis is nothing new. Just ask ex-Bank of Japan (BoJ) Governor Masaaki Shirakawa, the man who battled a 'green swan' – extreme financially disruptive events resulting from climate-related risks – before the term was even coined by the BIS in 2020.

On 11 March 2011, a magnitude 9.1 earthquake struck off the northeast coast of Honshu, Japan, which triggered a six-minute tsunami that decimated entire towns and caused a nuclear disaster. With waves as high as 40 metres, the defensive sea walls of the Fukushima Daiichi nuclear power plant, located along the coast, collapsed. Emergency generators were knocked out by the force of the tsunami, resulting in the meltdown of its core reactors and emission of dangerous radiation. As the death toll rose in the thousands and losses in the billions, the ensuing sell-off in Japanese stocks sent the yen to an all-time high. Japan was battling a climate-triggered financial crisis.

Working with other central banks, Governor Shirakawa and his team sold as much yen as required on the foreign exchange market to stabilise the currency. On the first business day after the disaster, the BoJ provided JPY21.8 trillion in liquidity, four times larger than its largest daily liquidity provision since the Lehman Brothers crisis, ensuring that banks could keep on lending. It instructed financial institutions to accommodate the withdrawal of deposits even when depositors had lost passbooks or certificates of deposit, providing three times the usual amounts of cash to people in affected areas. The BoJ also doubled government bond purchases under its asset purchase programme to JPY10 trillion. These raced measures reassured financial markets and prevented a spill over to other global markets.

Recounting the experience just 30 days after the deadly tsunami, Shirakawa said: "In the week following the earthquake, rumours spread mainly among some foreign financial institutions that Tokyo financial markets would close. While hard to believe, there was also a groundless rumour that the Bank of Japan would move its computer centre to Osaka. Extreme anxiety can in itself induce self-propagating market reactions. Fortunately, such rumours gradually dissipated.

On the first business day after the disaster, the BoJ provided JPY21.8 trillion in liquidity, four times larger than its largest daily liquidity provision since the Lehman Brothers crisis, ensuring that banks could keep on lending. It instructed financial institutions to accommodate the withdrawal of deposits even when depositors had lost passbooks or certificates of deposit, **PROVIDING THREE TIMES THE USUAL AMOUNTS OF CASH TO PEOPLE** in affected areas.

"If the financial and settlement systems as a whole had ceased to function normally, the adverse effects on people's lives and economic activity probably would have been even greater. The robustness of the financial system that we have seen this time was attributable to the hard work and solidarity of the people involved after the earthquake struck. I would also like to point out that the steady efforts of those involved in normal times, such as in developing business continuity plans and carrying out street-wide disaster exercises, greatly contributed to this robustness."

Solidarity – is it present in the global push for climate finance?

MEETING IN THE MIDDLE

The word 'adulting' – nominated as one of the most creative words of 2016 – is a humorous way of describing the act of doing basic, grown-up stuff. Things like showing up on time, owning a problem, or taking responsibility.

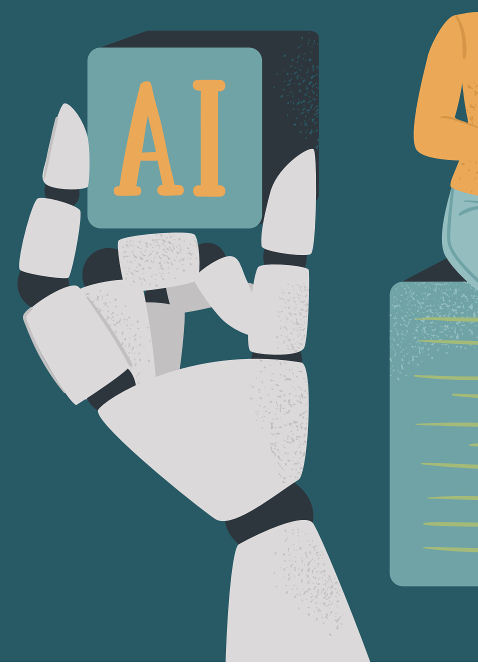
Being a grown-up also means being the voice of reason. It entails asking questions such as: What signal does it send to others when the biggest among us walk away from RtZ or GFANZ? Can we hold diverse opinions and still negotiate at the table? Can we meet in the middle?

This is a crucial adulting moment for banks. Although there are no prescriptive answers, there is however, a better way forward.

Will the adults in the room please stand up. ✱

■ *Angela SP Yap is a multi-award-winning social entrepreneur, author, and financial columnist. She is Director and Founder of Akasaa, a boutique content development and consulting firm. An ex-strategist with Deloitte and former corporate banker, she has also worked in international development with the UNDP and as an elected governor for Amnesty International Malaysia. Angela holds a BSc (Hons) Economics.*

CAREFUL, YOUR BIAS IS SHOWING



By Julia Chong

IF YOU'RE INTO AI, THIS ONE'S FOR YOU.

In Luxembourg, it wasn't until 1972 that a woman could open a bank account or apply for a loan in her own name without her husband's signature. Thus, women as a population are unlikely to be well represented in historical Luxembourgian banking datasets.

In recent times, Luxembourg's financial regulator, *Commission de Surveillance du Secteur Financier,* warned market players of bias in artificial intelligence (AI) systems, including the use of historical data such as the above if it has not been debiased before it is used to train intelligent systems.

The white paper, *Artificial Intelligence: Opportunities, Risks and Recommendations for the Financial Sector,* provides this example. Suppose a developer creates an AI-based credit scoring algorithm for a bank using historical data. Without taking into account the history of banking legislation in the coding of the algorithm, the modern women of Luxembourg could likely be disadvantaged by unfavourable credit scores compared to men. This is because in the past, women applicants were not granted many loans and unless the algorithm was adjusted to account for the dataset bias that existed prior to 1972, the automated credit score could disproportionately penalise women in the form of higher interest rates, fewer product options, or even denial of access to financial services.

The paper also highlights that "complex models may result in a lack of transparency for customers, to which it would be difficult to explain why a credit request was rejected…Also, if high volumes of credit decisions are automated, errors eventually included in the model would be amplified. Similarly, if a few models developed by external providers gain large adoption, design flaws or wrong assumptions contained in the models may have systemic effects."

The commission also highlights that

The paper also highlights that **"COMPLEX MODELS MAY RESULT IN A LACK OF TRANSPARENCY FOR CUSTOMERS,** to which it would be difficult to explain why a credit request was rejected...Also, if high volumes of credit decisions are automated, errors eventually included in the model would be amplified.

under the EU's General Data Protection Regulation, customers have the right "not to be subject to a decision based solely on automated processing".

Here, we see that even though it is possible to automate judgments to speed up simple banking processes such as credit scoring, risks can arise from a number of sources. In certain jurisdictions, consent is also a prerequisite.

Bias is built into our human DNA and bleeds into all aspects of our creation, including autonomous products and systems. It is not possible to eliminate bias, but we can mitigate it by being self-aware and observing basic standards of care.

BIAS IN THE CHAIN

In *Mitigating Bias in Artificial Intelligence: An Equity Fluent Leadership Playbook*, published by the Center for Equity, Gender and Leadership at the Haas School of Business at the University of California, Berkeley, there are various points at which bias can enter the AI value chain:

+ **Dataset:** Data is assumed to accurately reflect the world, but there are significant data gaps, including little or no data coming from particular communities and data is rife with racial, economic, and gender biases. A biased dataset can be unrepresentative of society by over or under-representing certain identities in a particular context. Biased datasets can also be accurate but representative of an unjust society. In this case, they reflect biases against certain groups that are reflective of real discrimination that the particular group(s) face(s).

+ **Algorithm:** Bias can creep in when defining the purpose of an AI model and its constraints, when selecting the inputs it should consider or when selecting the inputs the algorithm should consider to find patterns and draw conclusions from the datasets. An algorithm can also contribute to discriminatory outputs, irrespective of the quality of the datasets used, depending on how it is evaluated.

+ **Prediction:** There is potential for inaccurate predictions and bias if an AI system is used in a different context or for a different population from which it was originally developed or if it is applied for different use cases from which it was originally developed/operationalised. AI systems can be used or altered by organisations or individuals in ways that can be deemed as discriminatory for certain populations. This can be due to bad actors getting a hold of and using the technology. In other cases, it may be less overt and subject to debates over fairness. For AI systems that support human decision-making, how individuals interpret the machine's outputs can be informed by one's own lived experience.

I SPY WITH MY LITTLE EYE

One of the more insightful interviews in recent times on debiasing AI took place at EmTech Digital 2022, MIT Technology Review's annual conference on AI. The work of Dr Nicol Turner Lee, Director of the Center for Technology Innovation at the Brookings Institution, has been steadily gaining ground. As a vocal advocate for more enlightened AI, her goal is to squeeze inequality out of the equation by reminding scientists and practitioners to be honest.

"I tell everybody you need a social scientist as a friend. I don't care who you are – a scientist, an engineer, a data scientist. If you don't have one social scientist as your friend, you're not being honest to (sic) this problem, because what happens with that data? It comes with all of that noise and despite our ability as scientists to tease out or diffuse the noise, you still have the basis and the foundation for the inequality.

"So, one of the things I've tried to tell people [is that] it's probably okay for us to recognise the trauma of the data that we're using. It's okay for us to realise that our models will be normative in the extent to which there will be bias, but we should disclose what those things are.

"That's where my work in particular has become really interesting to me…What part of the model is much more injurious to respondents and to outcomes? What part should we disclose that we just don't have the right data to predict accurately without some type of risk to that population?"

The discussion invariably led to the subject of regulating the risks of AI. This question, posed by an audience member, reflects the frustration of developers and innovators who battle with less tech-savvy bureaucrats: "How do we engage and help legislators understand the real risks and not the hype that is sometimes heard or perceived in the media?"

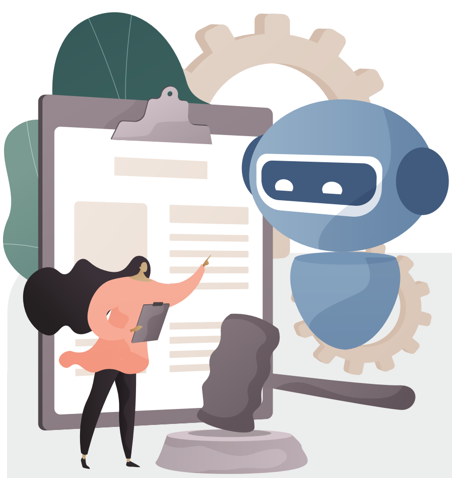
Dr Turner Lee's response: "I think you're right that policymakers should actually define the guardrails, but I don't think they need to do it for everything."

"I think we need to pick those areas that are most sensitive, what the EU has called 'high risk'. Maybe we might take from that some models that help us think about what's high risk, where should we spend more time, and potentially with policymakers, where should we spend time together?

"I'm a huge fan of regulatory sandboxes when it comes to co-design and co-evolution of feedback…but I also think, on the flip side, that all of you have to take account for your reputational risk."

'LIGHT TOUCH' IS OUT OF TOUCH

Views of how AI should be supervised are very similar to discussions about regulating fintech. Commenting on the fast-and-loose minting and volatile trading



REGULATORY GUIDANCE ON ETHICAL AI DEVELOPMENT

Common principles	Applicable standards/laws	How do regulatory expectations for AI differ from traditional models?
RELIABILITY/ SOUNDNESS 	• Basel Core Principles (BCP) 15. • Insurance Core Principles (ICP) 16, 17. • Basel Committee on Banking Supervision (BCBS) Principles for Effective Risk Data Aggregation and Risk Reporting. • Minimum requirements for the use of internal ratings-based (IRB) approach for credit risk, internal models approach (IMA) for market risk, stress testing, technical provisions valuation.	Similar expectations as traditional models (e.g. model validation, defining metrics of accuracy, updating/retraining of models, ascertaining quality of data input). However, AI models have added dimension and should be viewed from the perspective of avoiding causing harm (e.g. discrimination) due to inaccurate decisions arising from inherent bias.

of cryptocurrency, Eswar Prasad opined in his recent *FT* article *Crypto Poses Serious Challenges for Regulators,* that "when an industry clamours for regulation, it typically craves the legitimacy that comes with it, while trying to minimise oversight. That is the biggest risk regulators must guard against — giving the crypto industry an official imprimatur while subjecting it to light-touch regulation."

During the 2018 International Monetary Fund (IMF)/World Bank Bali Fintech Agenda, whilst President Joko Widodo was in favour of a "light-touch safe harbour" approach to ensure fintech and entrepreneurs were not curbed in their innovations, the then IMF Managing Director Christine Lagarde was sceptical.

"I am a little bit concerned when I hear…talk about the 'light touch'," she said, "because it reminds me of the soft-touch regulation we had just before the crisis in 2008."

"We point very directly to the risks of, what I would call as a former lawyer, 'forum shopping'. In other words, if there is no international cooperation, if there is no adherence to the Bali [Fintech] Agenda key elements, then there is a risk that somewhere, somehow, the regulatory environment will be conducive to an abuse of the system. It will be the leak through which unwanted, unnecessary business is being conducted."

Lagarde, and others such as then Bank of England Governor, Mark Carney, propounded that regulation, especially in high-yield and innovative sectors in fintech, should be proportionate to its risks. Proportionality in banking regulation promotes stability, whilst keeping regulatory burden and compliance costs at a minimum. It is in a constant tug-of-war with 'light touch' reforms that do not shield citizens from financial instability and bank bailouts.

If banking has emerged relatively unscathed by the Covid-19 pandemic, it is because of decades-long reforms under the Basel framework that are anchored in the concept of proportionality. Perhaps what could be made clearer to developers and innovators is that regulators are not expected to be subject matter experts; they exist to maintain the soundness and safety of the financial system on behalf of their citizens.

Supervisory authorities are concerned with specific challenges, such as defining the tiering criteria for applicable laws, achieving a level playing field, and minimising regulatory arbitrage. The truth is that it is incumbent upon developers to do their due diligence and not wait for a prescriptive rules-based regime to decide what's right and what's wrong.

After all, isn't that what autonomy is about? ✱

■ *Julia Chong is a content analyst and writer at Akasaa, a boutique content development and consulting firm.*

The key difference between regulatory requirements for traditional and AI models is the stronger emphasis for the latter on human responsibilities in order to prevent discrimination and other non-ethical decisions. The existing guidance, issued by the Bank for International Settlements in August 2021, is summarised below to ensure banks set higher standards for themselves as well as their service providers. More information is available in the BIS policy paper, *Humans Keeping AI in Check – Emerging Regulatory Expectations in the Financial Sector*, by Jermy Prenio and Jeffery Yong.

Challenges	Possible solutions
• Lack of rigour in data cleaning. • Inaccurate, incomplete or biased source data leading to unreliable or biased results. • Data source may not be generalised for the intended target consumer groups. • Lack of regular and timely updates and output reviews. • Existing regulatory requirements on model validation may need to be adjusted to accommodate certain ML techniques. • Striking the right balance between an algorithm's simplicity and its performance. • Overly onerous regulatory requirements to 'prove' the accuracy of an algorithm may not be achievable. • Data poisoning attacks involve altering training data sets used to build a predictive ML algorithm in order to manipulate its results. Such cyber breaches could lead to unreliable ML results and potentially become systemic.	• Supervised machine learning (ML) requires constant human feedback so that it can apply its trained 'knowledge' to produce reliable results. If the context changes, the training data set will need to be updated so that the algorithm can be retrained to produce reliable results. • Unsupervised ML requires timely updates and reviews. • The patterns or relationships revealed need to be assessed by a human expert. • Significant changes to internal models used by financial institutions typically require supervisory re-approval. • Tailor the intensity of governance measures to the impact of a given AI use case. • Emphasis is on the importance of technical human expertise overseeing the AI/ML framework. • Increased use of AI/ML in business processes by financial institutions needs to be supported by a sound cyber resilience framework.

Common principles	Applicable standards/laws	How do regulatory expectations for AI differ from traditional models?
ACCOUNTABILITY	• BCP 14, 15. • ICP 7, 17. • BCBS Corporate Governance Principles for Banks. • Minimum requirements for the use of IRB for credit risk, IMA for market risk, AMA for operational risk, stress testing, technical provisions valuation.	Similar expectations as general accountability or governance requirements, but human involvement is viewed necessary. AI models must have in-built "external accountability" to ascertain that data subjects (prospective or existing customers) are aware of AI-driven decisions and have channels for recourse.
TRANSPARENCY	• ICP 17. • Minimum requirements for the use of IRB for credit risk, IMA for market risk, stress testing, technical provisions valuation.	Similar expectations as traditional models, particular on explainability and auditability. AI models are also expected to perform external disclosure (e.g. data used to make AI-driven decisions and how the data affects the decision) to data subjects.
FAIRNESS	• ICP 19. • Common Framework for the Supervision of Internationally Active Insurance Groups Standard 7.2a. • Consumer protection laws in some countries explicitly address fairness concerns as described in AI-related issuances (i.e. prevent/address discriminatory outcomes).	Stronger emphasis in AI models. Expectations on fairness relate to addressing or preventing biases in AI models that could lead to discriminatory outcomes, but otherwise 'fairness' is not typically defined.
ETHICS	• BCP 29. • ICP 5, 7, 8. • BCBS Corporate Governance Principles for Banks. • BCBS Principles for the Sound Management of Operational Risk. • BCBS Principles on Compliance and the Compliance Function in Banks. • Financial Stability Board Toolkit for Firms and Supervisors to Mitigate Misconduct Risk.	Stronger emphasis in AI models. Ethics expectations are broader than 'fairness' and relate to ascertaining that customers will not be exploited or harmed, either through bias, discrimination or other causes (e.g. AI using illegally obtained information).

Challenges	Possible solutions
• Data accountability becomes less clear at lower levels of the hierarchy. • The human-in-the-loop or human-on-the-loop safeguards could give rise to new governance-related risks. • Interactions with external service providers through licencing of AI systems and procurement of data (e.g. credit scores) could impose constraints on financial institutions arising from intellectual property rights imposed by such providers. • Over-reliance on external providers could also lead to commercial capture and dependency risks, particularly given increasing cross-selling of digital services by big techs, making it difficult for a financial institution to insource the skills and expertise when needed under a business continuity scenario.	• Recruitment, training, and retraining of staff with specialist expertise. • Upskilling of boards and senior management with explicit accountability for AI deployment.
• If a model is not transparent, it will be difficult to assess its reliability, performance and fairness. • Difficult to establish accountability if it is unclear which components of the algorithm are causing errors, especially when using off-the-shelf solutions that automate decision-making. • Some ML algorithms such as deep learning and neural networks are often 'black boxes'. • Difficulty in explaining complex ML algorithms in a way that can be understood by a supervisor. • Erosion of consumer confidence or dissuade customers from using AI/ML powered financial solutions. However, the Monetary Authority of Singapore has pointed out that excessive transparency could create confusion or unintended opportunities for individuals to exploit or manipulate AI/ML models.	• Supervisors need to upskill their staff to be conversant with ML techniques. • Firms need to make more efforts to explain their ML models in an understandable way. • Assess understanding of the general concept of the model by board members – if this can be understood by non-technical board members, they will most likely be understood by supervisors as well. • Firms should strive to use explainable algorithms even if this is at the expense of model performance. • Where there are no viable alternatives (e.g. processing of images, videos or texts), firms can use alternative governance measures such as enhanced human oversight.
• Lack of universally accepted definitions of these terms. • Regulations that require exercise of sound human judgment may make it challenging to implement AI/ML. • Unfair or unethical AI implementation could have profound implications on consumers, which include financial exclusion and consequential destruction of livelihoods.	In general, AI governance principles or guidance on fairness and ethics require human-in-the-loop or human-on-the-loop.

MORAL REASONING: HOW DO WE GET TO THE RIGHT DECISIONS?

By Bob Souster

Understanding how individuals are influenced and what drives their actions (or inactions) hold immense importance for us in banking.

An overwhelming majority of bankers want to do what is right, for their employers, for the community, for society as a whole and for themselves. An industry that has been built on the trust and confidence of others has to take this as a given. But while we hope to take decisions and actions that reflect goodness, how do we arrive at our decisions about right and wrong? This article considers moral reasoning. It examines some of the factors that influence the thinking of individuals about their decisions. It is not about whether a decision is right or wrong, but the process through which the decision is taken.

INTUITION

The simplest view of moral reasoning is that there is no reasoning involved at all and that, as human beings, we intuitively know whether something is right or wrong. There may be multiple influences such as parents, friends, teachers, social environment, religion and countless other factors. These have been examined exhaustively by sociologists, many of which write of socialisation, and by psychologists, who are concerned with how the mind works and its impact on behaviour.

Enlightenment writers such as David Hume believed that concepts of morality were based on the perceptions of individuals and were akin to emotions. Three hundred years later, Jonathan Haidt supported Hume's simple view by writing of 'moral intuitions'. Yet, even in Hume's time, not all authorities agreed that morality relied on instinct. Immanuel Kant, for example, believed that there were universal laws that should always apply, and that these 'maxims' should form the basis of duties or obligations to others.

There is no conclusive evidence as to whether our decisions are driven by instinct or logical processes. Many bankers find themselves in situations in which they have to make snap judgments reflecting what they genuinely believe to be right. Is this through a finely-tuned sense of justice instilled through knowledge and judgment built from experience, or do their minds subconsciously follow a process?

COGNITIVE MORAL DEVELOPMENT

Theories of cognitive moral development considered moral reasoning as a process. Most of the theories relating to this approach were formulated by carrying out empirical research, such as by asking people questions and assessing their responses. Jean Piaget studied how cognitive processes developed

Figure 1: Kohlberg's theory of moral reasoning

LEVEL One	LEVEL Two	LEVEL Three
STAGE **Pre-conventional**	STAGE **Conventional**	STAGE **Post-conventional**
INFLUENCES The individual is concerned with self-interest, focusing on external rewards and punishments.	INFLUENCES The individual is concerned with the expectations of others: initially family, friends and peers, later by other influential stakeholders in their lives.	INFLUENCES The individual takes decisions more autonomously, based on principles of right and justice and independently of external influences.

APPROACH
Ethic of Obedience

RATIONALE

Concerned with rights, duties and obligations, or following the rules. Steare regards this (in its most rigid form) as synonymous with Kohlberg's pre-conventional stage. A powerful driver is fear.

APPROACH
Ethic of Care

RATIONALE

Concerned with the consequences of our actions and bringing about outcomes that reflect the greater good or least harm (utilitarianism). Steare saw this as manifesting itself at conventional stage (authority and social order maintaining orientation) but also post-conventional stage (social contract orientation). A powerful driver is empathy.

APPROACH
Ethic of Reason

RATIONALE

Concerned with virtues, principles and values such as wisdom and self-control. Steare aligned this with Kohlberg's post-conventional stage (universal principles). A powerful driver is reason.

Figure 2: Steare's theory

from childhood to adulthood. He believed that children were mainly influenced by rules made by influential people in their lives, or even by God. These rules were rigid and would often create notions of causation, such as 'naughty behaviour will result in punishment'. In this way, Piaget fused the duties (which arise from rules) with consequences of breaking the rules. Piaget believed that as the individual matured they would enter the autonomous phase, when it would be important to consider the underlying intentions of an individual, an acceptance that different people may have their own interpretations of morality and in some cases rules should be broken if appropriate to do so.

Piaget's theory paved the way for research by Lawrence Kohlberg, who developed his theory of moral development by posing ethical dilemmas to children of various ages and examining their responses. He concluded that individuals would apply different reasoning processes as they matured through three generic stages (**Figure 1**).

Kohlberg's theory posits that individuals move through these stages sequentially but at any given time may make judgments and take decisions based on any of the three stages.

During the deregulation of the 1980s, when banks were growing rapidly and becoming more sales-driven enabled by a 'soft touch' regulatory environment, it was possible for an able and ambitious person to make a name for themselves by meeting and exceeding their targets, just as less precocious contemporaries might have been more fearful of the negative consequences of failing to perform. In both cases they exhibit pre-conventional characteristics, being driven by perceived rewards and punishments respectively. Over two decades later and in the aftermath of the global financial crisis of 2009–2011, bankers were more likely to consider the expectations of others, notably government, regulators and their employers, as banks adopted more conservative, risk averse policies and the demands of regulators changed radically. This reflects conventional reasoning. However, one problem with generic theories is that, by definition, they do not apply to all people or situations. For example, it might be argued that whistleblowers who risked (and in some cases sacrificed) their careers on matters of principle took the high ground by considering right and justice above all, clearly demonstrating post-conventional reasoning.

Kohlberg's theory is not without critics, who have pointed out that his research base was narrow (all male subjects, small control groups, all in the USA). Carol Gilligan, a contemporary of Kohlberg, developed a parallel theory which postulated that women adopt different reasoning to men and are more inclined towards an 'ethics of care'.

INTEGRATING THEORIES OF ETHICS WITH MORAL REASONING

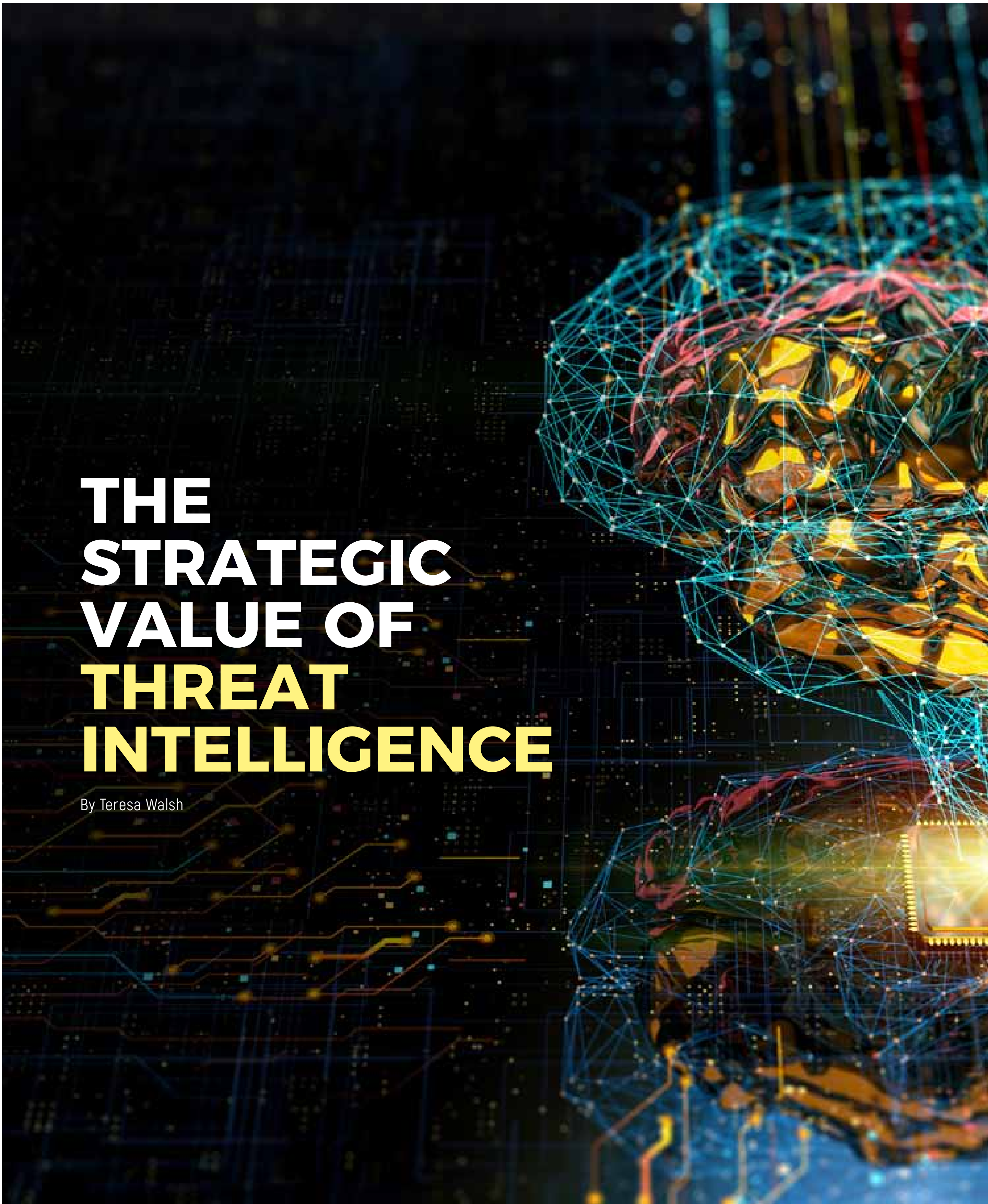
Drawing on the work of classical Greek philosophers and Enlightenment writers, as well as more contemporary research such as that of Kohlberg, Roger Steare developed an integrated and data-led approach to how individuals arrive at ethical decisions. His early findings were based on bringing together three approaches to ethics: virtues; duties; consequences. Steare's three typologies are described in **Figure 2**.

Steare's theory is a powerful attempt to bring together several theories of ethics. It is also built on practical research, as he built his data from inputs collected from thousands of online questionnaires.

CONCLUSIONS

We will never arrive at a definitive answer to the question, "How do we arrive at ethical decisions?". The theories and concepts discussed briefly in this article offer clues and indicators of how individuals are influenced and the factors that drive their decisions and actions, and sometimes their inactions. However, the discussion has important implications for us in the world of banking. When we assess new recruits, when we seek to influence the culture of our organisation and promote exemplary practices, when we try to promote noble behaviours and deter malevolent behaviours, we need to understand the multiplicity of factors both within and outside our control. ✱

■ *Robert (Bob) Souster is a Partner in Spruce Lodge Training, a consultancy firm based in Northampton, England. He lectures on economics, corporate and business law, management, corporate governance and ethics. He is the Module Director for 'Professional Ethics and Regulation', a core module of the Chartered Banker MBA programme at Bangor University, Wales.*



THE STRATEGIC VALUE OF THREAT INTELLIGENCE

By Teresa Walsh

Compared with other forms of threat intelligence like human or signals intelligence that have been used by nation-states as part of national security and defence for many decades, cyber intelligence is still a relatively new concept.

Cyber intelligence, particularly in the private sector, tends to focus on technical data such as threat actors' technical capabilities and objectives to combat cyber threats at the tactical level. However, businesses, especially those in high-risk sectors such as financial services, can and should apply learnings from the public sector to utilise threat intelligence at higher levels to better manage cyber risks and fortify business resilience.

EXPANDING BEYOND THE TACTICAL

Cyber threat intelligence possesses vast utility, yet many organisations today are not harnessing threat intelligence to its fullest potential, instead focusing only on low-level, tactical use cases. Ideally, however, organisations can and should use threat intelligence analysis to detect both immediate and long-term threats, prioritise mitigation strategies, refine and sharpen long-term security postures, and focus on activities that further cyber resilience – all of which can greatly support a company's success.

This reimagining and reorientation of how organisations make use of threat intelligence is necessary because threat intelligence holds immense value at multiple levels – tactical, operational, and strategic.

+ **At the tactical (and lowest) level,** threat intelligence detects and provides information on imminent cyber threats, enabling security teams to make better tactical decisions to secure an organisation's defences.

Intelligence used at the tactical level focuses on the 'what' — what information an organisation needs to know while responding to security incidents, often involving the techniques, tactics, and procedures used by threat actors.

This intelligence is typically technical in nature and obtained directly from threats detected inside an organisation's systems or from external sources that can impact tactical decisions, such as intelligence shared by another organisation about a threat that they have recently encountered.

+ At the operational level, threat intelligence empowers cybersecurity stakeholders by shedding light on cyber threat actors' motives as well as tactics, techniques, and procedures and helps cybersecurity professionals better understand the threat actor's decision-making process.

At the operational level, tactical intelligence can be used as building blocks to help expand the threat picture to the malicious actor behind the attacks and the arsenal of tools leveraged against victims. Operational intelligence analysis looks at the campaign level, examining priority threats and ongoing challenges in real time.

+ At the strategic level, threat intelligence informs top-level stakeholders in the business, such as board members and C-level executives guiding decision-making on investment, risk mitigation, and other high-level decisions.

The use of strategic intelligence focuses on uncovering the 'how' — how an organisation defends itself and its overall cybersecurity posture. Unlike tactical intelligence, strategic intelligence provides a high-level view of the threats faced by an organisation and is human analysed and human readable.

Just as national intelligence estimates are created to influence some of the highest levels of government, so too can threat intelligence be used at the strategic decision-making levels of private firms to arm stakeholders such as IT, risk, and business continuity managers with actionable information on not only what could cause operational disruption but the probability of the specific firm being impacted, and even the cost of certain types of attacks. This in turn helps these stakeholders gauge their risk appetite more accurately and prioritise investments.

> The intelligence cycle is a step-by-step process that **INFORMS THE DEVELOPMENT AND EXECUTION OF EFFECTIVE THREAT INTELLIGENCE COLLECTION**, analysis and dissemination, and is critical to generating insightful and actionable intelligence for stakeholders.

In order to ensure the application of threat intelligence meets strategic ends, a company must integrate the planning and direction stages of its intelligence cycle, keeping in mind its risk management needs and strategy when collecting and analysing data or information. The intelligence cycle is a step-by-step process that informs the development and execution of effective threat intelligence collection, analysis and dissemination, and is critical to generating insightful and actionable intelligence for stakeholders.

The next step is to establish priority intelligence requirements. For the cybersecurity team, these can often be technical or generic, such as 'malware' or 'DDoS (distributed denial of service) attacks'. These on their own may not be very meaningful to risk managers who care about how this could lead to the failure of IT networks and subsequent availability to customers, as well as subsequent

compliance risks. However, when these are mapped onto the firm's risk frameworks, they can provide an answer to the question of "so what?". In turn, this allows risk managers to truly understand how vulnerable they are to specific threats and allocate resources accordingly.

TOWARDS INTELLIGENCE-SUPPORTED BUSINESS RESILIENCE

With the rise of third-party risk, organisations are more prone to cyberattacks due to external failures or deficiencies. This is compounded by concentration risk, as many firms around the world rely on the same small pool of third-party vendors for essential services. On top of this, the proliferation and evolving nature of cyber threats mean that a successful attack or breach is now nearly inevitable — and organisations must ensure they are equipped to continue operations even when under attack. In other words, organisations must become operationally resilient. Threat intelligence, and its effective use, is crucial to this process.

> With the rise of third-party risk, organisations are more prone to **CYBERATTACKS DUE TO EXTERNAL FAILURES OR DEFICIENCIES.** This is compounded by concentration risk, as many firms around the world rely on the same small pool of third-party vendors for essential services.

To combat these attacks against commonly used third parties, an organisation's cyber threat intelligence team must know who its critical suppliers and partners are and how they interact with the business. The intelligence team must also interact and collaborate across departments so that intelligence can be integrated into data collection requirements, threat monitoring, and analytical products.

For example, resilience and exercise managers can engage in a tabletop exercise to simulate a third-party supplier cyberattack; or chief information security officers can collaborate with peers on addressing concentration points of common suppliers at a sector-level effort to ensure their security levels are adequate.

As third-party risk increasingly impacts both compliance and reputation, an efficient and effective risk management strategy is critical. Using strategic threat intelligence analysis to detect threats, prioritise mitigation strategies, and target resilience activities can help companies leverage existing threat intelligence resources to a much greater value in protecting the company and assuring the operational resilience that customers, shareholders, and regulators increasingly demand. ✱

■ *Teresa Walsh is the Global Head of Intelligence, Financial Services Information Sharing and Analysis Center (FS-ISAC). FS-ISAC is the member-driven, not-for-profit organisation that advances cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve. Founded in 1999, the organisation's real-time information sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defence. Member financial firms represent USD100 trillion in assets in more than 75 countries.*

FINANCIAL CRIME ON THE NEW FRONTIER

SCAMS ASSOCIATED WITH CRYPTOCURRENCY

By Eva Crouwel, Wesley Gibbs, Willem du Plessis, and Nicole Botha

Avoiding crypto crime requires cooperation.

CRYPTO CRIME

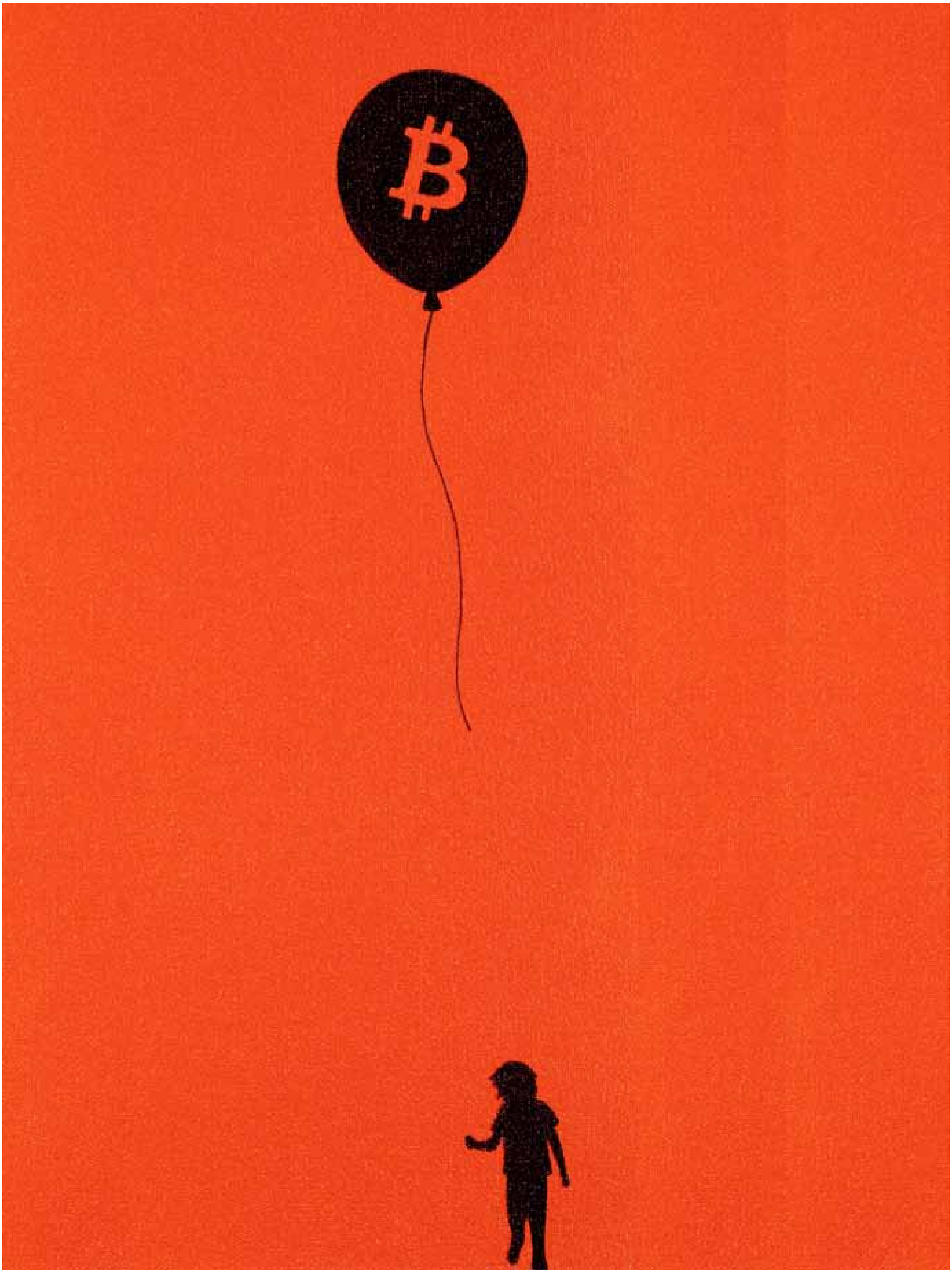
Over the last few years, the adoption of cryptocurrency has been on the rise globally, with specifically high adoption rates within the Asian and African markets. However, with the rise in this adoption a shadow side has emerged; that of financial crimes pertaining to cryptocurrency. Most prevalent amongst these crimes, according to a 2022 report issued by blockchain monitoring provider Chainalysis, were cybersecurity related crimes (such as hacks) and scams. In fact, according to the *2022 Crypto Crime* Report compiled by Chainalysis, scams were once again the largest form of crypto-based crime (by transaction volume) with in excess of USD7.7 billion worth of virtual currency misappropriated from victims worldwide.

When looking specifically at increased scams within the Asia region, the struggle is very real indeed. Recent publications, for example by the Malaysian Securities Commission, recorded a total of RM5.2 billion in losses with over 7,200 reported cases to the Malaysian government from the period May 2020 to May 2022. The contrast is stark; where 1,800 cases were reported in 2020, by 2021 this figure had grown to 3,500 reported cases and 2022 looks to be on track for similar numbers.

Recognising the economic opportunities afforded by these advancements to the general public and enabling the rapid expansion and adoption of (different types of) cryptocurrency, whilst also ensuring the safety of consumers within this new market is a nontrivial task.

INVESTMENT SCAMS

Investment scams can be considered the largest bane of all financial scams. Investment scams at their core promise big payouts with minimum risks. Promises of quick money and guaranteed returns make these scams attractive to a wide range of consumers.



The combination of increased interest from consumers with regard to financial planning and investments, the created perception of 'great wealth' achieved by early adopter crypto millionaires and the new technology that is brought on by cryptocurrency, creates a perfect storm for exploitation. This perfect storm has recently been further amplified by the effects of the Covid-19 pandemic. The pandemic has played a significant role in the economic downturn for a large portion of consumers, resulting in a need for immediate and significant financial relief.

Investment scams specifically target a victim's naivety and exploit their search for 'easy money' while ending up losing a significant amount of funds. More often than not, victims are coerced into investing in order to gain significant returns in a relatively short period of time. These are known as 'get rich quick schemes' and exploit the still prevalent understanding of consumers that cryptocurrency is a means of substantial wealth generation in a limited amount of time. The most common result is that victims are required to pay more and more to a scammer in order to see a return, before they finally realise that they have lost all that they invested.

Investment scams are hard to detect at an early stage and particularly difficult to combat as victims are often convinced that the scammer or their organisation is reputable and reliable and refuse to believe any alternative.

RUG PULLS

With the introduction of cryptocurrency, scams have gained significant sophistication. Scammers no longer solely rely on one specific method to lure their victims, but have found ways to use a combination of techniques in an effort to launder funds or scam investors out of their money, leaving individuals with the 'rug' pulled out from under them.

Rug pull scams rely on the information asymmetry between investors and fraudulent blockchain technology developers to defraud investors on development projects. As projects emerging on the decentralised blockchains have become more popular, it has provided fraudsters with the opportunity to capitalise on the lack of understanding of the projects' underlying source, validity, and trustworthiness of its founders.

The year 2021 saw the most famous example of a rug pull with the SQUID token (inspired by the dystopian Netflix series called *Squid Games*). The value dropped by 99.9% after the creators made off with an alleged USD3.4 million.

Investment scams specifically target a victim's naivety and exploit their search for 'easy money' while ending up losing a significant amount of funds. More often than not, **VICTIMS ARE COERCED INTO INVESTING IN ORDER TO GAIN SIGNIFICANT RETURNS IN A RELATIVELY SHORT PERIOD OF TIME.** These are known as 'get rich quick schemes' and exploit the still prevalent understanding of consumers that cryptocurrency is a means of substantial wealth generation in a limited amount of time.

MONEY MULE SCAMS

A relatively new phenomenon is the money mule scam. These come in a variety of subsets of scams, but their shared trait is that individuals or 'mules' are used to unwittingly aid the laundering of illicit proceeds by further obfuscating the source of funds.

In certain of these scams, individuals are lured into extravagant schemes where the so-called trader or broker (the scammer) supplies liquidity for the individual "to have a kick-start on their investment and make more money than they can imagine" or "to help a friend".

This forms a tempting proposal for the young, the cash-strapped, and the lonely as well as the elderly demographic who are preyed on to make an extra buck or gain a 'friend' for the use of their attached crypto wallets and/or bank accounts.

Over the past two years there has been a significant increase in money mule scams, including what is known as a 'safe account' scam. This is where the scammer impersonates a bank employee and reaches out to an individual to report that there has been fraud on their account. Unquestionably distressed, the impacted individual easily parts with personal information and identification documentation in order for the scammer to create a so-called 'safe account'.

The scammer then requests the victim to move their funds to the safe account specified by the scammer. The result is the scammer having access to an account in the victim's name, opening up the possibilities for fund laundering, as well as access to the victim's funds.

The resulting fallout for the victim establishes significant barriers as well as financial loss. In addition to losing their funds, victims are often blacklisted by financial institutions and their respective relationships terminated for facilitating the laundering of stolen funds.

ELDERLY SCAMS

Over the last years, elderly scams have been on the rise. These scams specifically target senior citizens as they may have access to considerable savings, are often technologically illiterate, may experience age-related ailments and are generally less likely to report incidents over fear of losing their independence or being perceived as inept.

Elderly scams often see victims losing significant amounts of critical funds, such as pension funds or retirement savings, with no way of recouping their losses. The scams are reliant on and target the vulnerabilities attached to elderly individuals in order to extract personal information and/or secure undue financial benefit.

Scammers make use of various platforms and a variety of techniques in attempting to gain the trust of victims. Thereafter, the individual is more susceptible and can easily be coerced into disclosing valuable personal information or accepting assistance (initiating an account takeover). Sadly, scammers often include family members or individuals known to the victim.

Often, the combination of the age of the consumer, their use of cryptocurrency and the volume and value of their transactions can function as a red flag.

> Scammers make use of various platforms and a variety of techniques in attempting to gain the trust of victims. Thereafter, **THE INDIVIDUAL IS MORE SUSCEPTIBLE AND CAN EASILY BE COERCED INTO DISCLOSING VALUABLE PERSONAL INFORMATION OR ACCEPTING ASSISTANCE** (initiating an account takeover). Sadly, scammers often include family members or individuals known to the victim.

ROMANCE SCAMS

As more and more people have turned to online dating, apps and social media, scammers have seized the opportunity. These scams, commonly referred to as 'sweetheart scams' or 'catfishing' occur when a scammer adopts a fake online persona in order to gain a victim's affection and trust. The scammer deceives the victim, using the illusion of a romantic relationship or close friendship to exploit and/or steal from the individual.

As these scams typically extend over long periods, victims are often fleeced out of large sums of money and end up losing both a significant emotional relationship as well as their funds.

RISK MITIGATION

When thinking about risk mitigation pertaining to scams, it is important to consider that scams occur within an ecosystem that consists of consumers and traditional financial institutions as well as cryptocurrency enablers.

As consumers, when considering any activity within the cryptocurrency

ecosystem, it is imperative to be reminded of the adage, "if it's too good to be true, it probably is". Cryptocurrency can be used as a means of investing, but large promised returns, especially when structured in an 'investment plan' or 'club' should be considered a major red flag.

Thorough research is imperative when considering making any financial investments, including cryptocurrency investments. Consumers should not rush investment decisions and often scammers pressure victims into making deposits before they have time to think it through. The use of brokers, account managers, traders, sponsors, agents and other people that offer to trade cryptocurrency on a consumer's behalf should specifically be avoided.

Consumer education is an essential part of the role cryptocurrency enablers have to play to reduce the asymmetrical information positions that scammers take advantage of. Cryptocurrency providers should put emphasis on educational content when interacting with consumers and invest in making relevant content easily accessible to those interested in their products. In addition, customer segmentation and targeted protection, sometimes by even denying the product to specific consumer segments altogether, is a strong mitigation measure that should be put in place. Having a deep understanding of customers, their interactions with the products and how these behaviours correlate to specific customer vulnerabilities is crucial in preventing scams.

Lastly, defences against scams can be found in the relationship between traditional financial service providers and cryptocurrency enablers. While the cryptocurrency enablers may be providing the end service to the customer, thus facilitating funds being sent to a scammer, the financial service provider, such as the customer's bank, will have sight and a form of control over transactions going to cryptocurrency enablers. Through regular interactions and collaboration, financial institutions can flag both vulnerable and suspicious customers as well as questionable transactions to the cryptocurrency enabler. In addition, joint transaction prevention lists can be drawn up, specifying the outright denial of transactions that meet certain criteria. This creates a strong advance warning system as well as a control system that serve to protect the shared consumer within the ecosystem.

Lastly, defences against scams can be found in the **RELATIONSHIP BETWEEN TRADITIONAL FINANCIAL SERVICE PROVIDERS AND CRYPTOCURRENCY ENABLERS.** While the cryptocurrency enablers may be providing the end service to the customer, thus facilitating funds being sent to a scammer, the financial service provider, such as the customer's bank, will have sight and a form of control over transactions going to cryptocurrency enablers.

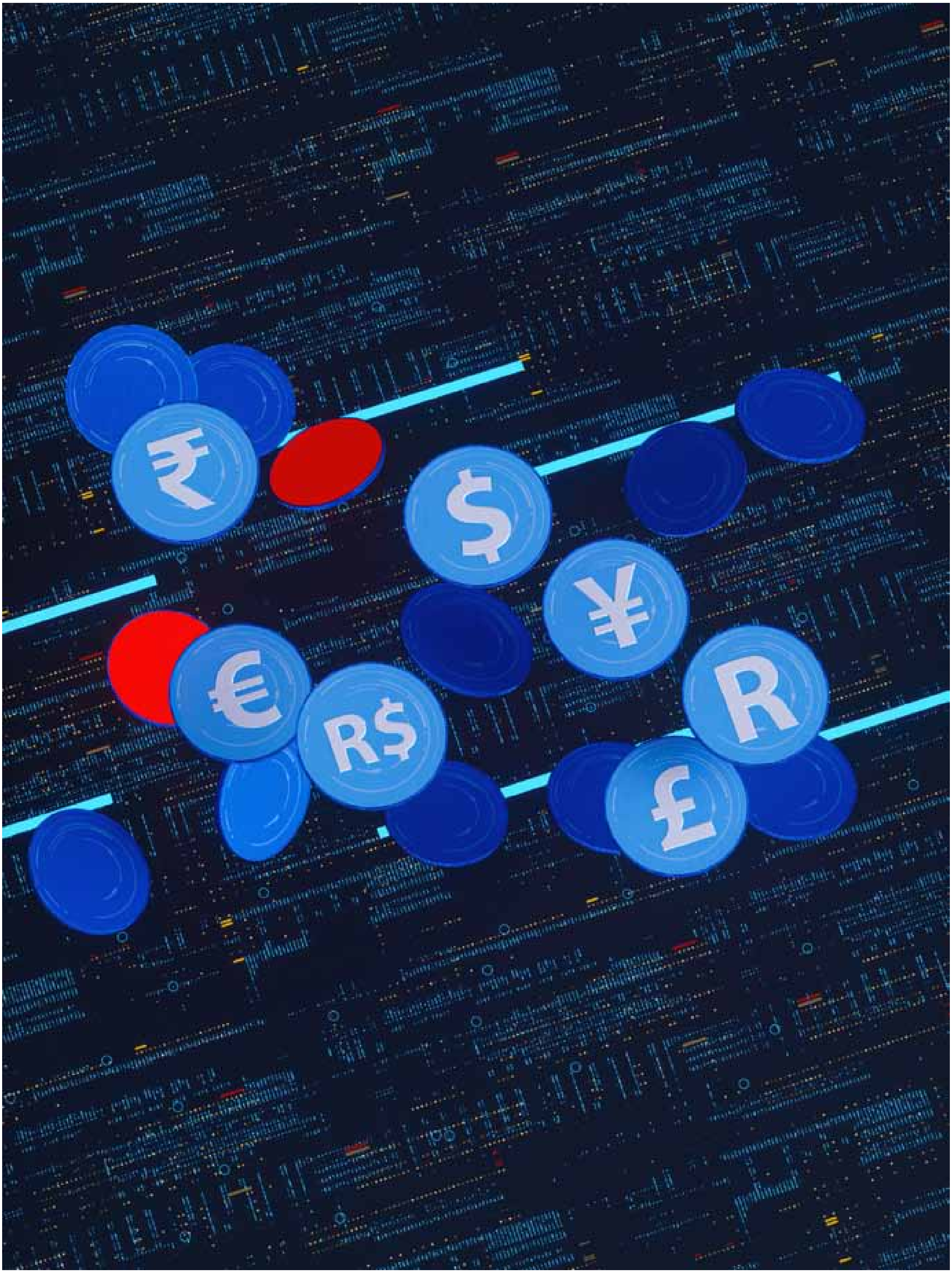
Cryptocurrency is here to stay but it cannot be denied that financial crimes are detrimental to consumer trust in both cryptocurrency as well as traditional finance. The adoption rate of cryptocurrency over recent years, as well as newly emerging technologies within the virtual/digital asset ecosystem present wonderful opportunities for the future of financial services and at the same time come with threats towards consumers in the use of this technology.

The ecosystem of financial services is one where traditional finance and cryptocurrency can and should co-exist. The curbing of financial crimes within cryptocurrencies should be seen as a shared challenge between consumers, traditional financial service providers, cryptocurrency providers and enablers as well as government agencies (such as regulators and law enforcement). Joining the dots between traditional finance and cryptocurrency enablers will be key to intentional and determined efforts to curb financial crime, increase trust and protect consumers within the financial ecosystem. ✱

■ *Eva Crouwel LLM CAMS is an experienced financial crime professional with over a decade of experience. She currently works as the Global Head of Financial Crime for Luno, a global cryptocurrency platform.*

■ *Wesley Gibbs, Willem du Plessis, and Nicole Botha are Financial Crime Investigators at Luno.*


MYCO ID: 201201039737
REGISTERED HRD CORP TRAINING PROVIDER
ASIAN BANKING SCHOOL
"THE LARGEST SPECIALISED PROVIDER OF QUALITY BANKING TRAINING PROGRAMMES IN THE ASEAN REGION"
The Asian Banking School (ABS) offers leading-edge and industry relevant training programmes that cover a comprehensive list of banking areas. They are designed and developed in-house by our Specialist Training Consultancy Team who are all HRD Corp Certified Trainers or in collaboration with strategic learning partners that includes some of the top business schools in the world. Many of these programmes are HRD Corp claimable with 88 approved and available so far.
To find out more about how ABS can help your organisation with training programmes that are HRD Corp Claimable :
Visit www.asianbankingschool.com | Email training@asianbankingschool.com
Scan the QR Code to download a copy of our HRD Corp claimable programmes brochure



AN OVERVIEW OF CRYPTOCURRENCY REGULATIONS IN ASIA PACIFIC

By Dow Jones Risk & Compliance

REGULATORY ACTIVITIES ARE SET TO INCREASE ALONG WITH COMPLIANCE NEEDS.

Since the fall of Mt. Gox, regulators around the world have been examining the risks and challenges associated with cryptocurrencies. A now-defunct Tokyo-based cryptocurrency exchange, Mt. Gox was hacked in 2014 for 850,000 bitcoins (at the time worth almost USD500 million), which raised important regulatory questions. While the Tokyo District Court approved a case-related rehabilitation plan last year, the questions of jurisdiction, the financial definition of cryptocurrency and virtual asset service providers (VASPs), security protocols and anti-money laundering/countering financing of terrorism (AML/CFT) measures continue to be discussed among regulators and crypto players.

Amidst escalating needs to counter ransomware attacks and to prevent virtual currencies from being used for sanctions evasion, regulators, led by the Financial Action Task Force (FATF), are scrambling to regulate the crypto industry. It is therefore imperative for businesses to keep abreast of relevant regulations in order to mitigate financial and legal risks in the ever-evolving crypto world.

REGULATORY LANDSCAPE

FATF

Although the FATF's recommendations and guidance are not legally binding, they are recognised international standards and many countries are working to comply with them. In October last year, FATF updated the guidance for virtual assets (VAs) and VASPs. Some key recommendations for crypto businesses are:

- VASPs are to be subject to the same relevant FATF measures that apply to financial institutions. This means that customer due diligence, including identification of beneficial owners and politically exposed persons (PEPs), enhanced due diligence for high-risk jurisdictions, record keeping, sanctions screening and reporting of suspicious transactions, are required for crypto businesses.
- VASPs need to be licenced or registered where they are created through an existing or new purpose-built mechanism. VASPs where services can be accessed from a different jurisdiction may also be requested to register in the hosting jurisdictions.
- While the idea is not new, the FATF

takes the view that the so-called travel rule (Recommendation 16) — the obligation to obtain, hold and transmit required originator and beneficiary information immediately and securely throughout the payment chain — applies to VA transfers. VASPs such as exchanges and custodial wallet service providers should be required to capture certain information, such as the names of the originator and the beneficiary, addresses and identification numbers in line with customer due diligence (CDD) requirements for any transaction over USD/EUR1,000.

SINGAPORE

Singapore is attempting to continue its success in branding itself as Asia's crypto financial hub by introducing strict regulations while maintaining a tax-friendly environment and driving blockchain innovation. This initiative was recently reiterated by Ravi Menon, Managing Director of the Monetary Authority of Singapore (MAS): "The licencing process is stringent because we want to be a responsible global crypto hub, with innovative players but also with strong risk management capabilities."

Pursuant to this, the city-state has implemented these key measures:

- After the Financial Services and Markets Bill was passed earlier this year, intermediary companies that want to process digital payment tokens are required to obtain a licence if they are established in Singapore but provide services outside of the country. This brings the country's licence requirement in line with the latest FATF guidance.
- Under the Payment Services Act, the crypto licensee will need to satisfy certain requirements such as having a permanent place of business, record keeping and having a "fit and proper" person, as well as being in good financial standing. In addition, they will also be subject to AML/CFT requirements. These include due diligence exercises, transaction monitoring, record keeping and reporting of suspicious transactions related to AML/CFT risks.
- The travel rule implemented through MAS Notice PSN02 on *Notice to Holders of Payment Service Licence (Digital Payment Token Service),* which came into effect in January 2020, imposes more stringent requirements for information gathering (e.g. the identification number and residential address for transactions exceeding SGD1,500 in value).

HONG KONG

Hong Kong is also establishing a robust regulatory regime for crypto players. The Legislative Council has accepted that Hong Kong's regulatory regime for VASPs should be "more rigorous and comprehensive (than those in Singapore, the UK and Japan)". This has been achieved through amendment of the existing Anti-money Laundering and Counter-terrorist Financing Ordinance (AMLO). These changes come into effect on 1 March 2023.

- Currently, the Securities and Futures Commission (SFC) can only regulate VA trading platforms through a voluntary licencing mechanism; trading services in non-security tokens fall outside of the SFC's jurisdiction. Although voluntary licensees are required to have AML/CFT procedures, a reputable external market surveillance system, full insurance coverage, due diligence on VAs and good financial standards, the opt-in scheme has limited reach and carries no enforcement. For example, many major crypto currencies, such as bitcoin and ethereum, are not considered 'securities' and fall outside of the SFC's jurisdiction. There are certain requirements for fund managers of VA discretionary investment accounts investing in cryptocurrencies that are not considered securities.
- The Hong Kong Monetary Authority (HKMA) traditionally oversees AML/CFT matters related to financial institutions but does not regulate cryptocurrencies, as they are a 'virtual commodity' rather than legal tender. However, the HKMA has publicly warned of the highly speculative nature of virtual commodities and urges extra caution when considering transactions or investments.
- From March of next year, VA will be defined as 'digital

- representation of value' under the amended AMLO and the SFC will have wider licencing and enforcement powers.
- Firstly, anyone seeking to operate a VA exchange will need a licence, whilst those who participate in the opt-in scheme will be exempt. Similar to financial institutions, licence applicants will need to pass a 'fit and proper' test assessing experience and qualifications as well as previous convictions.
- Secondly, the applicant will need to appoint at least two SFC-approved responsible officers to ensure AML/CFT compliance requirements are met under Schedule 2 to the AMLO. This includes CDD, the travel rule and record keeping.
- Lastly, the SFC will be given robust supervisory powers such as inspection, investigation and imposition of administrative sanctions in the case of non-compliance. For example, operating a VA exchange that is open to the public of Hong Kong without a licence could incur a fine of HKD5 million and seven years' imprisonment. In case of AML/CFT non-compliance, responsible officers may be liable to a fine of HKD1 million and two years' imprisonment.
- Currently, the VASP regulatory regime is limited to those providing services to professional investors, but is likely to expand to retail investors. Peer-to-peer platforms where transactions are taking place privately, as well as stablecoins, are excluded.

JAPAN

Japan suffered yet another crypto heist in 2018 when Coincheck, a Tokyo-based cryptocurrency exchange, was hacked for over USD500 million in digital assets. The attack highlighted not only security concerns but also wider sanctions implications. According to cybersecurity firm Group-IB, the North Korean state-sponsored Lazarus Group was behind the attack. Lazarus Group has since been sanctioned by the United States for participating in North Korea's cyber operations to support illicit weapon and missile programmes. Japan has traditionally been a crypto-friendly country; cryptocurrencies have been recognised as property since 2017 under the Payment Services Act (PSA) and crypto investments are taxed as 'miscellaneous income'. Given the recent scandal, the country is developing a new set of regulations:

> Japan suffered yet another crypto heist in 2018 when Coincheck, a **TOKYO-BASED CRYPTOCURRENCY EXCHANGE, WAS HACKED FOR OVER USD500 MILLION** in digital assets. The attack highlighted not only security concerns but also wider sanctions implications.

- In terms of registration, Crypto-asset Exchange Service Providers (CAESPs), including traditional exchanges, brokering service providers and custodial wallet providers, must register with the Financial Services Agency (FSA). To do so, applicants need to have a physical presence in Japan, JPY10 million in capital, a sound corporate structure and an appropriate compliance programme. For a foreign company to register, it must have a licence equivalent to the requirements under the PSA and a resident representative in Japan.
- The registration process includes a questionnaire, which covers a broad range of topics such as system security, privacy protection, AML/CFT measures (PEP and sanctions screening and auditing processes), and measures to counter anti-social forces.
- The FSA issued a second warning last year against Binance, the largest global crypto exchange, for operating in Japan without a licence.
- As a Specially Permitted Business under the Act on Prevention of Transfer of Criminal Proceeds, CAESPs are required to perform a Know Your Customer (KYC) procedure for any transactions over JPY100,000. Transactions over JPY2 million are considered high risk and require additional checks, such as additional KYC documentation and confirming the source of income.
- Following the Russian invasion of Ukraine, Japan revised the Foreign Exchange and Foreign Trade Act to prevent cryptocurrencies from being used to evade sanctions. Accordingly, CAESPs are now prohibited from executing crypto transfers unless they confirm that the recipient is not on a sanctions list.

- The travel rule was introduced 1 April 2022 with full implementation from 1 October 2022 by the Japan Virtual and Crypto assets Exchange Association (JVCEA), the self-regulated body established under the PSA. During the transition period, CAESPs initiating a transaction with receiving VASPs must obtain, keep and share the originator's name and address and the name of the beneficiary. The beneficiary's address and transaction purpose must be shared beginning October. Even when there is no requirement to pass the information to the receiving VASP (e.g. the receiving VASP is located in a jurisdiction with no travel rule), an individual risk assessment will also be required before approving the transaction.

SOUTH KOREA

In South Korea, after the amendment of the Act on Reporting and Using Specified Financial Transaction Information came into effect in September 2021, domestic and offshore VASPs are required to register with the Financial Intelligence Unit and comply with various AML/CFT obligations. A couple of key points should be considered for crypto compliance:

- Security tokens representing ownership of a business or financial interest are currently treated like other VAs, but the Financial Services Commission has recently proposed to amend the Capital Markets Act to incorporate Security Token Offerings (STOs). This may result in more oversight and regulation of tokens, similar to securities.
- When VASPs provide exchange services involving fiat currency, customers must establish a real-name bank account at the same bank with a VASP. VASPs are also required to verify the identity of their customers through their banks, which will bring more traceability in the market.

REGULATORY PITFALLS

While crypto regulations diverge across Asia and the world, it is important to determine what type of business entity you are defined as in your home jurisdiction because this serves as the basis for various regulatory requirements. Similarly, it is important to understand where your customers are, as their consumer protections may restrict your activities in their jurisdiction.

- Keep up with technology. Blockchain technology is still in its early stages. Non-fungible tokens (NFTs) are growing in popularity. While the FATF does not recognise NFTs as VAs, it cautions that a case-by-case approach is necessary when it is used for payment or investment purposes. There are many gray areas regulators have not clarified, such as the treatment of stablecoins.
- Keep up with regulatory changes. Crypto regulations are still fragmented; countries are trying to regulate virtual activities by redefining existing regulations or through new regimes. Last month, the EU agreed to expand the travel rule and synchronise regulations across member states. Crypto firms will be required to declare information on their environmental and climate footprint. More regulatory oversight is expected globally in the coming years.
- As highlighted in a recent Goup of Seven statement, crypto assets are already covered by existing sanctions regimes. The US has already penalised a mining firm for facilitating sanctions evasion by Russia and a crypto exchange for facilitating ransomware actors' transactions. Due to their global reach, crypto businesses should be aware of US sanctions as well as domestic sanctions.

OUTLOOK

For crypto firms, it is important to detect regulatory risks early, establish a corporate governance framework and have a playbook ready. They can also learn from traditional financial institutions with decades of experience in risk management training, establishing auditable workflows, screening, reporting and managing reputational risks. Consumer sentiment is also important, as calls for stronger oversight came from consumers who witnessed the recent market crash. As more rogue nations and criminals exploit the crypto world, regulatory activities will increase along with compliance needs. ✱

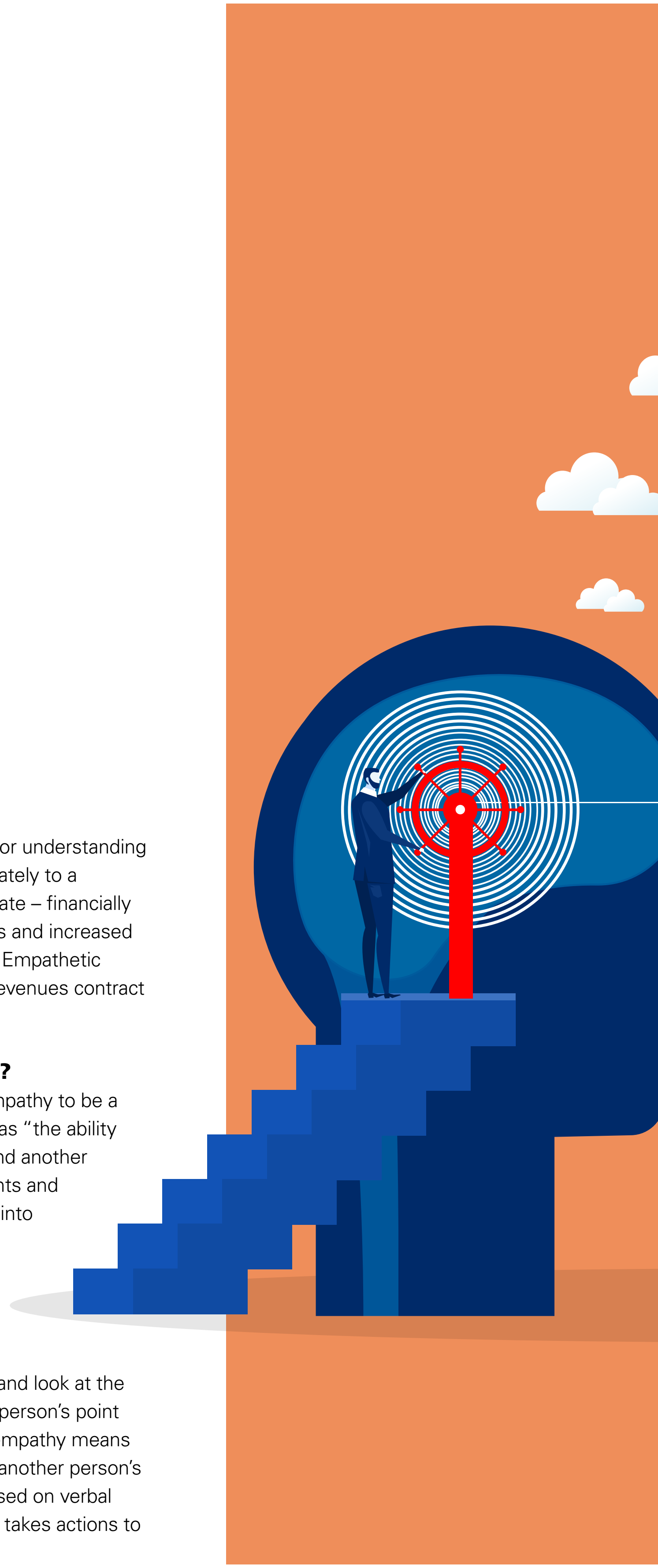
■ *Dow Jones Risk & Compliance is a global provider of risk data, integrated technology solutions and due diligence services covering anti-money laundering, anti-bribery and corruption, sanctions and international trade compliance.*


AICB
ASIAN INSTITUTE OF CHARTERED BANKERS
Gain a competitive advantage with the Chartered Banker status

Why Banks Should Bet on Empathy

By Marjorie Giles

Listening pays off in the long run.



In 2020, Accenture conducted a global study comprising 125 senior executives from the top five banks. The subject was Empathetic Banking. A questionnaire was devised to identify these leaders as either Empathetic Banking Leaders, Contenders, or Laggards. Their answers were then compared against the banks' self-reported non-financial performance metrics (customer loyalty, newly acquired customers, customer trust, employee engagement scores, employee productivity, and customer cost-to-serve) and, finally, plotted against their financial performance.

The objective was to quantify how much of a role customer-directed empathy had played in their service model and had they seen the returns of their investment in this new approach.

The results, captured in the firm's 2021 report titled *Banking on Empathy: Engaging with Customers in a More Human Way,* showed that banks led by Empathetic Banking Leaders – individuals with strong capabilities for understanding and responding appropriately to a customers' emotional state – financially outperformed their peers and increased revenue by 1.3%, whilst Empathetic Banking Laggards saw revenues contract by 0.6% on average.

WHAT IS EMPATHY?

Researchers deem empathy to be a personality trait defined as "the ability to identify and understand another person's feelings, thoughts and situation", categorising it into two types: cognitive and affective.

Cognitive empathy, also known as 'perspective taking', is the ability to step out and look at the situation from the other person's point of view. High cognitive empathy means that a person can 'read' another person's needs and intentions based on verbal and non-verbal cues and takes actions to address the issue.

Affective empathy, however, is more emotion-laden. The individual responds to the other person's emotional state without having experienced the emotion themselves. This induces feelings of concern but also contagion, where one mimics the other person's gestures or experiences stress when the other person is fearful or anxious.

In the business world, many see empathy as a disadvantage, an indication that you are just not cut out for the job. However, numerous studies in marketing and sales literature point to just the opposite: the best salespeople are also the most empathetic listeners.

Research proves that empathy is a predictor of trust and determines the quality of their relationship with the financial institution. In the customer's eyes, the question, "Do I trust my banker?" is nearly indistinguishable from "Do I trust my bank?". Studies, such as one published in the *International Journal of Bank Marketing* by Omar S Itani and Aniefre Eddie Inyang from the University of Arlington, Texas, reinforce why banks should never underestimate the power of the personal touch, something which digitalisation cannot fully replace. Their 2016 paper, *The Effects of Empathy and Listening of Salespeople on Relationship Quality in the Retail Banking Industry,* posits that "empathy and listening have been found to be important determinants of customer satisfaction and, thus, relationship quality (RQ). The objective is to examine the relationship between a bank's salespeople's empathy and listening, and the customers' RQ with the bank from the perspective of the customers."

The authors posit that exhibited empathy by retail banks' salespeople raises the RQ between customer and the bank: "When salespeople practice effective listening skills, they are more likely able to accurately assess verbal and non-verbal cues from their customers and to respond appropriately, enabling them to build rapport with customers".

"[Lucette B] Comer and [Tanya] Drollinger [in their 1999 paper *Active Empathetic Listening and Selling Success: A Conceptual Framework*

BANKING IS BECOMING MORE RELATIONAL, NOT TRANSACTIONAL

Accenture's research, *Banking on Empathy: Engaging with Customers in a More Human Way (2021)*, outlines four steps on how banks can merge the human touch with technology.

ANTICIPATE THE CUSTOMER'S INTENT AT THE ZERO MOMENT OF TRUTH.

An empathetic bank anticipates customers' motions and intentions early in an interaction and adjusts its tone of voice and customer journey to their needs. The bank's ability to translate the customer intent at the zero moment of truth – that second when they might be researching which services, products, or advice they need to navigate a financial crisis or opportunity – into empathetic actions hinges on its ability to integrate data from different systems and sources on a single platform that works in real time.

This might sound like old news; banks for years claimed to understand the zero moment of truth and the importance of a single, real-time view of the customer. Yet Accenture's research reveals a gap between banks' belief in the importance of a single view of the customer and their success in reaching this outcome.

Only 20% said that they are able to update and evaluate sales and service interactions on an ongoing basis. Moreover, even though more than 90% of banks say that they use both internally and externally structured data to at least a moderate extent in their sales and service practices, only 12% of consumers think their bank's customised experiences are spot-on.

The shift towards digital channels offers an opportunity for banks to accelerate the implementation of a single view of the customer.

MAKE EMPATHY PART OF THE DIGITAL SKILLSET

Equip digital channels with technologies that enable an empathetic response. To provide an empathetic experience, a bank needs to understand a customer's emotional state. This is easier when the interaction takes place face-to-face with a skilled advisor, but it can be more challenging through digital channels. Banks that are leading on empathy through digital channels are increasingly tapping into technologies such as voice recognition, speech analysis and text analytics to better understand customers' emotions. These technologies can help interpret a customer's sentiment in the moment in much the same way as a skilled human agent would, improving empathy across channels by matching service responses to the customer's emotional rather than economic profile. The research shows that Empathetic Banking Leaders are twice as likely as Laggards to already be using these technologies to enable empathetic interactions at scale.

published in the *Journal of Personal Selling & Sales Management]* found that salespeople with effective listening skills can "develop and maintain long-term relationships with their customers". They also found that effective listening skills lead to an increase in customer satisfaction. Customer satisfaction with a salesperson after an interaction is based on an emotional state in which the customer assesses the quality of the interaction experience. Therefore, when customers perceive the salesperson as having effective listening skills, they are likely to have a positive assessment of the interaction with the salesperson.

Whether it is anticipating a customer's need when making a financial decision or making account holders feel that their opinions matter (a feeling that's increasingly lost in the 'noise' of remote banking), it pays for financial institutions to invest in upping the emotional quotient of their workforce.

GETTING SATISFACTION

Itani and Inyang suggest some ways to achieve satisfaction:

- When hiring new salespeople, bank managers should make sure that they assess the empathy and listening levels of prospective employees. Managers can use as a pre-employment screening test, the Toronto Empathy Questionnaire that assesses the empathy levels of applicants as well as the Interpersonal Listening in Personal Selling scale.
- Examples of volunteering and social activities that applicants have on their résumés can serve as

TRANSFORM CONTACT CENTRES INTO EMPATHETIC CUSTOMER CARE HUBS

Deliver a better contact centre experience on a greater scale. Making the contact centre the main focus of live customer interaction is a natural step towards a customer service model that scales better than serving customers through the branch network. There is a risk, however, that the empathetic touch could be lost as customers wait for service in long phone queues and interact with a different agent each time they contact the bank.

Leading banks are seeking to resolve this tension by transforming their contact centres into empathetic customer care hubs. This, in turn, means investing in capabilities that promote empathetic experiences by reducing call hold times and adding a personalised touch to the customer conversation. There are three levers banks can use to transform their contact centres into empathetic customer care hubs.

Firstly, empathetic banks will make human chat the primary way that customers interact with their contact centres. For instance, banking leaders are using artificial intelligence (AI) to match their customers with the best advisor for their emotional profile, which can increase retention, cross- and up-sell, and net promoter scores.

Secondly, empathetic banks will augment contact centres with digital capabilities to promote an empathetic banking experience without physical face-to-face interaction. AI virtual agents, for example, will help contact centre advisors provide relevant customer service as they manage growing contact volumes and also adopt the right tone of voice for the specific customer.

Finally, empathetic banks will combine resources from the back-office, service centre, branch, and contact centre into distributed contact centres. For instance, an investment advisor who is idle in a branch would be able to pick up a query from a customer who called the central contact centre seeking wealth management advice. This could help reduce holding times or to connect customers to the representative who is best qualified to help them with their requests.

REINVENT BRANCHES AS EMPATHETIC EXPERIENCE CENTRES

The branch of the future will be far from the most important distribution channel for most banks. However, the customer interactions that take place here will be among those that matter most to the customer's experience and perception of the bank. Indeed, banks with a traditional branch network still enjoy higher customer trust levels than pure digital players.

Some are reinventing their branches as hubs where customers and community members can learn, network, and connect in a comfortable and inspiring setting. Here, customer engagements might focus on improving access and financial inclusion. Banks might also use their branch footprint as decentralised offices for customer care representatives, or other service staff, enabling them to maintain a branch presence whilst downsizing their head offices.

Many are moving from a standardised, centrally controlled structure to a model where branch managers have more autonomy to respond to local needs, including the flexibility to adapt opening hours according to the needs of their communities and being accountable not only for branch-based sales and service but also for the digital customer base in their market.

Additionally, the skills mix at branches is under scrutiny. More than six in 10 banks in the survey agreed that 26% or more of their branch employees will need to be reskilled in the coming one to two years in order to meet higher service demands.

indicators of the 'other-orientation' of applicants, which can be a proxy of their empathy level.

- For current employees, banks should focus on the kind of training that enhances the self-efficacy of their salespeople. Individuals with high self-efficacy are more likely to consider work challenges and demands as things to be mastered; they also believe that they control more of the organisation's resources which makes them less likely to be affected by job demand stress.
- Other training should focus on attenuating the negative effects of stress on salespeople. Emotional intelligence can enhance interpersonal relationship building, which, in turn, can facilitate sales and help salespeople cope with the stress they face at work.

POST SCRIPTUM

The digitalisation of the banking sector should not be seen as separate from empathetic banking. In fact, it is imperative to acknowledge that the technological tools at our disposal – artificial intelligence, virtual reality, speech analytics, and other tools – cannot supplant human intuition, but can be deployed to assist bankers in making the customer journey more intuitive and emotionally satisfying. ✱

■ *Marjorie Giles writes for Akasaa, a boutique content development and consulting firm, and holds a Masters in Clinical Psychology.*

THE FOUR-DAY WEEK IS IMMINENT, ACCORDING TO EXPERTS

By Chartered Banker, UK

Alongside the influx of post-pandemic remote, flexible, and hybrid working options, will the financial services industry choose to embrace these controversial changes?

The world of work is far more jumbled than we typically acknowledge. For many industries, from medicine to hospitality and from retail to travel, the required hours do not fit neatly inside the traditional Monday-to-Friday pattern. Despite this truth – and some efficiency improvements facilitated by technology – we still largely commit to a working week born from the requirements of a century-old manufacturing industry. Is it time to reinvent the wheel?

In the US in 1926, businessman Henry Ford began to promote a 40-hour week, across five days. The six-day set-up wasn't giving workers enough opportunity to spend their wages. To counter unemployment caused by the Great Depression, North America officially adopted a five-day week in 1932. Across the water, John Boot, founder of British pharmacy Boots, began to close his factory on Saturdays and Sundays from 1934, enabling him to keep his staff employed on the same pay, without the need for redundancies. He noticed positive effects on productivity, and subsequent studies found a strong correlation between two-day weekends and output. In 1934, the UK made the five-day week official.

Today, similar studies are taking place, but it's the four-day week that's up for trial. Governmental and business support for the idea has been found in countries including Iceland, the UK, New Zealand, the US, and Ireland. Can this new approach work operationally within the financial services sector?

A QUESTION OF TRUST

The Covid-19 pandemic forced large parts of society to rearrange the way they work. For those in financial services, offices were largely closed; in-person meetings were replaced with Zoom calls; and some relaxation of corporate formality crept in. Millions of employees were forced to work from their bedrooms and kitchen tables as well as plan their time around the needs of their young children.

"When discussing the possibility of a four-day week, there were two questions that were typically raised pre-pandemic," recalls Andrew Barnes, Founder, 4 Day Week Global. "Can I trust my employees, and how do I measure productivity? Covid proved that people could be trusted to go home and work; and that presenteeism doesn't equate to output."

SAME PAY, FEWER HOURS

While there are variations on the concept of the four-day week, such as reducing hours and subsequently pay or condensing five days into four, these are being dismissed by 4 Day Week Global, one of the key organisations behind a number of the trials worldwide. Based in New Zealand, the organisation was set up after Barnes led successful trials in 2018 with his financial services company Perpetual Guardian. The system is based upon what has become known as the 100:80:100 model: 100% productivity, for 80% of the time, with 100% pay.

"It started with trying to work out why so many organisations struggled with low productivity. We asked, "What would happen if we gave staff the challenge to work smarter, rather than longer?" In return, they'd get the extra day off – provided output remained the same. What happened is that we simply got rid of unproductive time," says Barnes.

Advocates for the model claim it offers myriad benefits such as improved work-life balance, social, community and family benefits, and sustainability improvements.

PRODUCTIVITY ON THE UP?

The UK's Charity Bank, a financial organisation and social enterprise that supports the charity sector, has recently begun a six-month pilot of the scheme. For Chief Executive Officer (CEO) Ed Siegel, the hope is that productivity improvements achieved by each participating employee will enable output levels to be maintained while working one fewer day per week.

"On one level it's pretty simple. We're basically saying, 'You have a job description, or annual targets, and we expect you to continue doing the same thing but in four days per week instead of five.'" says Siegel.

"One of the crucial elements behind the 100:80:100 theory is that the three-day break makes you more productive. You come back refreshed and motivated, and ready to push through to the next weekend."

The largest UK business to commit to a four-day week is also a financial services organisation. Atom Bank moved all employees onto a four-day contract with no change in salary last year. The bank says it has seen no drop in productivity or output since making the change.

"Statistically, you're interrupted in an open-plan office every 11 minutes. The last two hours of the working day are the most unproductive," says Barnes. "A lot of this is about understanding that output is different from the hours you spend at work."

"Obviously, when you don't have everyone in the office, you have to work out how to measure productivity. This is about a mature, modern conversation between employer and employee."

A huge motivator behind both Charity Bank and Atom Bank's **CHANGE TO THEIR WORKING WEEKS LIES IN THE IMPROVEMENT OF EMPLOYEE WELL-BEING.** Due to the potential for significant reduction in sick days and absenteeism, this is thought to be something of a win-win for these financial organisations.

BEATING BURNOUT

A huge motivator behind both Charity Bank and Atom Bank's change to their working weeks lies in the improvement of employee well-being. Due to the potential for significant reduction in sick days and absenteeism, this is thought to be something of a win-win for these financial organisations.

A significant 55% of days taken off due to ill health in the UK is attributed to work-related stress, depression and anxiety. Atom Bank's staff surveys have suggested employees feel less stressed and look forward to their working day more since the shift to a four-day week. Pursuit Marketing, a Glaswegian business that made the change three years ago, report a 30% increase in productivity, with sickness at an all-time low.

With almost one-third of financial services and banking professionals planning to leave the industry due to high pressure, could this provide a solution to a problem that affects sectors such as financial services disproportionately: that of burnout, long hours, and employee ill health?

RECRUITMENT CRISES

Promoting the health and happiness of employees could also prove beneficial when it comes to attracting and retaining high-quality staff. Covid has accelerated discussions around work-life balance and job purpose. For an industry typically associated with tradition and corporate work practices, financial services organisations could find they need to modernise to remain competitive in the world of recruitment.

"There's much academic debate about to what extent there has really been this 'Great Resignation'. But whether this is true or not, you will certainly find evidence of widespread labour shortages and recruitment crises," says Dr Tom Calvard, Senior Lecturer in Organisation Studies, University of Edinburgh Business School.

"Nothing's more conservative than some areas of the financial services industry. Employers are going to have to come up with a new deal for employees if they want to recruit successfully."

For Charity Bank, competing with the bigger financial institutions was undoubtedly a huge motivator. "It's about making Charity Bank a better place to work and adopting a more modern-day approach to employment. If we are successful, we become a more attractive employer and compete better against mainstream commercial banks," says Siegel.

"These days, post-Covid flexible working is almost an expectation. I think some of the corporate CEOs that are insisting people get back to the office have missed a trick, and they're going to regret it."

Interestingly, Atom Bank reported a 500% increase in job applications since making the shift.

LEVELLING THE PLAYING FIELD

Improving inclusion and accessibility is another potential advantage of the reinvention of the working week. The financial services industry still has a long way to go on its journey to gender parity. Parental leave, flexibility for childcare, and gender pay gaps, all remain an obstacle to progress in the sector; overwhelmingly for women.

"Flexi-hours allow for the school run, or an extra day off enables everyone to spend more time with their families," continues Siegel. "And there's often a perception that if you're not full time then your opportunities for promotion will be limited. This certainly evens that playing field even more."

Similar ideas around inclusion can be applied to today's ageing population. As the workforce grows steadily older, could a reconfiguration of the working week be better suited to the needs of employees in later age?

"People are going to have to work longer. If you're looking ahead to a sustainable long-term career, working into your 60s and 70s, it could offer a solution to some of these problems," suggests Calvard.

OPERATIONAL CHALLENGES REMAIN

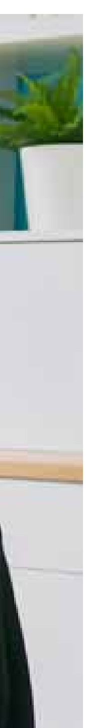
So far, it seems hard to argue against the idea of reinventing the working week. There are, however, a number of potential issues when it comes to implementation and logistics. Can the concept work in roles that require a 24/7 presence? In Gothenburg, Sweden, the answer was no. A nursing home trialled a version of reduced hours for the same pay, by shortening the working day to six hours. After two years, the costs of employing new staff to fill the rota were too high to continue.

In the UK, the Wellcome Trust scrapped plans to introduce a four-day week for its 800 head office staff after deciding that it was too operationally complex. The decision was taken after a three-month study found there were also negative effects on the well-being of some staff, who were trying to compress work into less time – increasing exposure to stress.

This is the type of feedback that Charity Bank is already monitoring. "I do know that some people are finding it easier to transition than others. Some people work long hours and are having a hard time getting things done in five days, let alone four," says Siegel. "There's a group [of people] who are saying they'd love to do this but aren't yet quite sure how to adjust their days and practices."

POLITICAL AND NATIONAL SUPPORT

The international governmental interest in this idea has been widespread. Iceland is heralded as a global leader in this space, having trialled reduced hours since 2015.



The UK is currently part of a pilot scheme involving 70 businesses nationwide, with the Scottish government offering explicit support. But there are some concerns about the repercussions a four-day week could have on overall societal inequality.

Critics cite the potential for a widening of the gap between lower-paid, gig or hourly work, and professional salaried employment. Many believe there is a need for political and institutional backing before the four-day week could be established universally.

"Certain elements, such as hybrid working policies, can be drafted relatively quickly or experimented with. But the length of a working week is more of an institutional issue," says Calvard.

"One of the biggest negatives is that, when looking at banking and other white-collar areas, employees are being offered the same money for less time at work – compare that to people on other types of contracts, hourly or otherwise, and the divide becomes clear."

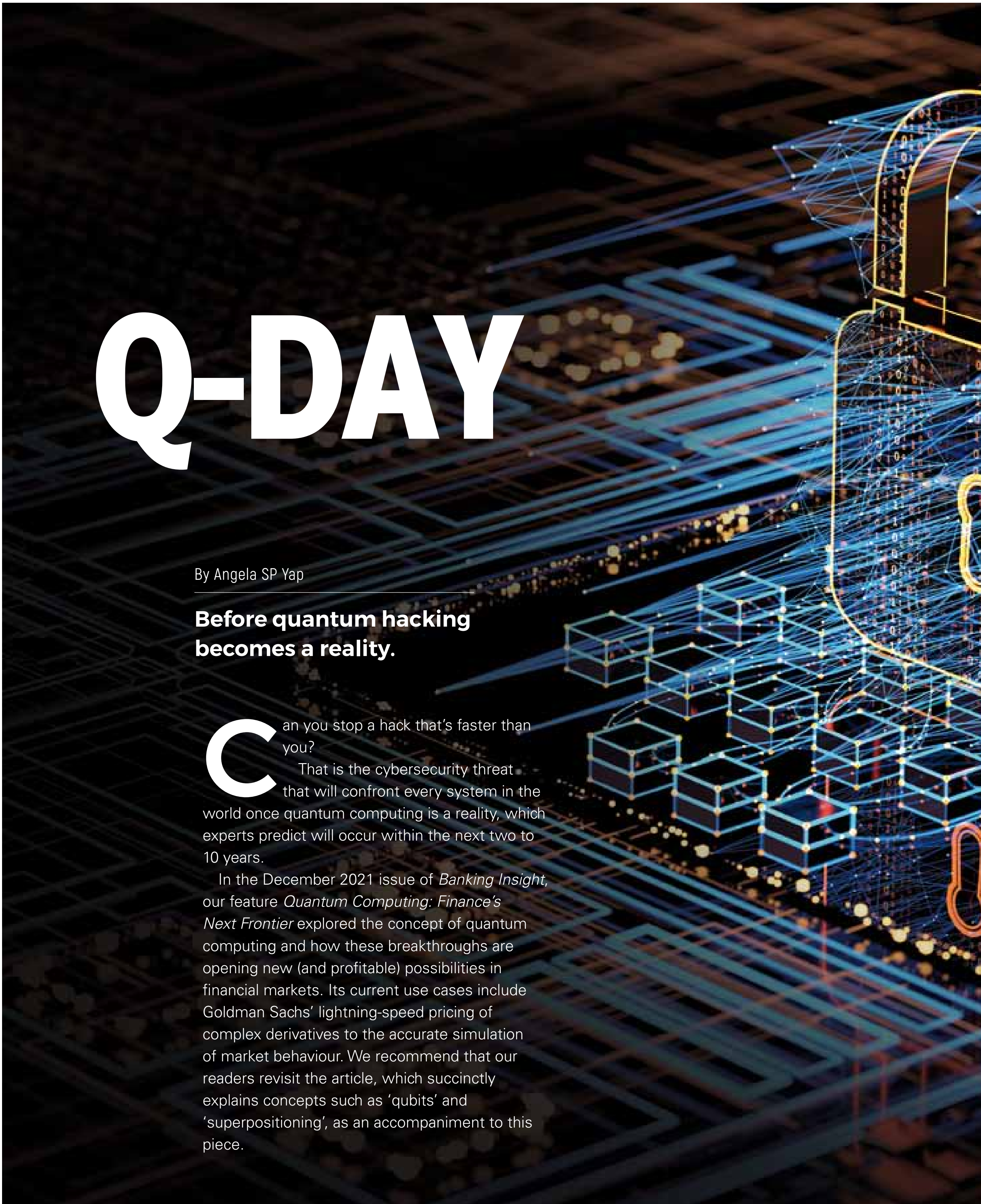
Indeed, employment statuses and the creation of a two-tier workforce are of a pressing concern, when for many, the hunt is for more hours, not less. For Asheem Singh, Director of Economy, Royal Society of Arts, the conversation needs to be more philosophical, as he said in a BBC interview in May 2019.

"The decision needs to be taken at a national level. The question is: are we prepared to make politically tough choices about whether we valorise leisure, and spending time with our families, as part of our economy and society?"

Whatever an individual's stance on the four-day week, what cannot be denied is that the financial services sector is faced with a growing recruitment challenge and must adapt to keep securing the best and brightest talent.

The Covid pandemic has catalysed a shift in working and living expectations. For many, there are big conversations to be had about some of life's bigger questions. A reinvention of the working week might be just over the horizon. ✱

■ *This article previously appeared in the Chartered Banker magazine, UK, Autumn 2022 edition.*



Q-DAY

By Angela SP Yap

Before quantum hacking becomes a reality.

Can you stop a hack that's faster than you?

That is the cybersecurity threat that will confront every system in the world once quantum computing is a reality, which experts predict will occur within the next two to 10 years.

In the December 2021 issue of *Banking Insight*, our feature *Quantum Computing: Finance's Next Frontier* explored the concept of quantum computing and how these breakthroughs are opening new (and profitable) possibilities in financial markets. Its current use cases include Goldman Sachs' lightning-speed pricing of complex derivatives to the accurate simulation of market behaviour. We recommend that our readers revisit the article, which succinctly explains concepts such as 'qubits' and 'superpositioning', as an accompaniment to this piece.

Quantum Day, or Q-Day in cybersecurity circles, refers to the day when the power of quantum computers will be harnessed to 'crack' secure codes that transmit sensitive information, such as digital signatures or trading data. Luckily for us, time is on our side. Code breaking on a quantum machine requires qubits (quantum bits) in the thousands, and most quantum computers currently work around 50 qubits. This is changing rapidly as technology companies and governments race to the finish line.

IBM, whose current capacity is reportedly a 127-qubit processor, has announced a roadmap to produce a 4,158-qubit quantum processor called Kookaburra by 2025. Google's Sycamore machine was in pole position until October 2021 when a team from the University of Science and Technology in China developed two machines, Jiuzhang 2 and Zuchongzhi 2.1, the former of which could compute calculations at least 100 trillion times faster than Sycamore.

China's national research and development spend increased by 7% in 2021 with a reported USD10 billion already invested in the field. It also holds more quantum technology patents than even the US, which trails with a dismal USD1.2 billion budget earmarked over a five-year period under the National Quantum Initiative Act 2018 and has spent only USD900 million thus far for the fiscal year 2022.

Private sector players are also getting into the game albeit, with smaller budgets. Zapata Computing, a Massachusetts-based quantum software company, reports that in 2021 the sector is pulling in serious private-sector dollars with 28% of global enterprises allocating seven-figure budgets, a turning point from the USD100,000 research and development budgets of the past. Its *First Annual Report on Enterprise Quantum Computing Adoption,* comprised of 300 leaders (chief investments officers, chief technology officers, other vice-president-level and above executives) from companies with turnover exceeding USD250 million and USD1 million computing budgets.

HACKING, BUT ON STEROIDS

Flush with investment dollars and with such grandiose machines already in the works, it is a bit surprising then that there hasn't been more discussion on countering the havoc that will ensue once cybercriminals get their hands on such machines and quantum hacking begins.

What takes conventional supercomputers hundreds of years to compute could be accomplished in a matter of seconds once quantum computing is fully realised. Think of it as the digital-day version of the code-breaking Bombe machine created in the 1940s by mathematical genius Alan Turing, which did the impossible by decrypting the German's Enigma code, securing vital intelligence for the British government. With quantum capabilities, the ability to crack existing codes will be in the milliseconds.

Already, 2022 is set to become the most lucrative ever for hackers who amassed USD3 billion in 125 hacks as at October, based on a tweet by blockchain intelligence firm Chainalysis. One of China's top cryptographers, Prof Jintai Ding of Tsinghua University, predicted at a forum in December 2021 that USD3 trillion worth of cryptocurrency assets will soon be vulnerable to hacking by quantum computers.

Quantum Day, or Q-Day in cybersecurity circles, refers to the day when the power of quantum computers will be harnessed to **'CRACK' SECURE CODES THAT TRANSMIT SENSITIVE INFORMATION,** such as digital signatures or trading data. Luckily for us, time is on our side. Code breaking on a quantum machine requires qubits (quantum bits) in the thousands, and most quantum computers currently work around 50 qubits.

There are two ways through which that will happen:

- **'Collect now, decrypt later' strategies.**
  Although hackers have yet to acquire the know-how or tech infrastructure to decipher information that is currently encrypted, this does not prevent them from acquiring and storing such information in preparation for a time when quantum computers can reliably break these security algorithms.

- **Outdated cryptography.**
  Much of the sensitive data exchange over the internet by banks are based on public-key cryptography. The idea is that information can be securely transmitted through the internet using a public key (comprising numbers, alphabets, symbols) to encrypt and securely transmit the message, and a second private key (a different set of numbers, alphabets, symbols) that is known only by the intended recipient is used to 'unlock' the message and read it. There are numerous types of public-key-exchange algorithms – RSA, elliptic-curve, Digital Signature Standard – some of which the world is slowly transitioning away from as these encryptions become more easily deciphered by classical computers. However, the looming threat of quantum hacking means that these keys, public and private, can be cracked faster and *en masse*.

CRACKING STUFF

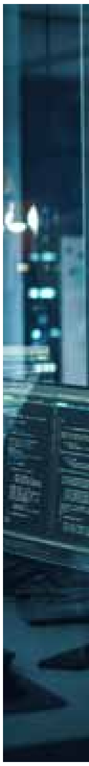
In quantum-resistant encryption, researchers often refer to Shor's Algorithm, named after Peter Shor, Professor of Applied Mathematics at Massachusetts Institute of Technology. It shows how a quantum computer should theoretically be able to break RSA (in use since the 1970s) and elliptic-curve keys, rendering current cryptographic systems vulnerable.

In his opinion piece, *Q-Day Is Coming Sooner Than We Think,* Arthur Herman, Senior Fellow at the Hudson Institute and Director of the Quantum Alliance Initiative, writes: "There's a growing consensus that this quantum threat is real; there's no agreement how long it will take before a quantum computer has the 4,000 or so stable qubits it will need to meet the requirements of Shor's algorithm for cracking those encryption systems.

In his opinion piece, Q-Day Is Coming Sooner Than We Think, Arthur Herman, Senior Fellow at the Hudson Institute and Director of the Quantum Alliance Initiative, writes: **"THERE'S A GROWING CONSENSUS THAT THIS QUANTUM THREAT IS REAL;** there's no agreement how long it will take before a quantum computer has the 4,000 or so stable qubits it will need to meet the requirements of Shor's algorithm for cracking those encryption systems.

"The fact that the [US] National Institute of Standards and Technology (NIST) won't have its quantum-resistant algorithm standards ready until 2024, and expects the rollout to space out for another five to 15 years, has helped to encourage complacency disguised as confidence. But new developments in quantum science suggest that this complacency is misplaced…it's probably going to be here sooner than even experts thought."

Indeed, the NIST's track record in this respect has been dismal. In August 2022, one of the four encryption algorithms it considered to be 'quantum resistant' – or safe from decryption by quantum computers – was embarrassingly decrypted by researchers using a good ol' Intel-chip laptop. The Belgians who cracked the code, Wouter Castryck and Thomas Decru, researchers at KU Leuven, made their code public together with details of the 2013 off-the-shelf laptop, and collected a nifty USD50,000 bounty from Microsoft, the company that developed the original encryption algorithm.



PANTS UP

What measures can leaders take to pre-empt quantum hackers from targeting their companies? Boston Consulting Group, in its article *Quantum Hacking is the Next Big Cybersecurity Threat. Here's How Companies Should Prepare for 'Y2Q',* recommend that companies should already cultivate what it calls 'crypto agility' in these four ways:

+ **Escalate this to the board and top management.** Companies must make cybersecurity a business priority. They must assign the responsibility for tracking developments in quantum computing to a team, led by a senior leader, such as the chief information officer or chief information security officer, that reports regularly to the board and top management. This will ensure that the focus is on corrective, not organisational, issues when quantum computing arrives. Doing this will be critical in sectors such as finance, where the risks are higher due to the nature of the business and its dependence on data. Some banks are already working with quantum computing companies on risk mitigation methods or have created a global organisation structure to deal with security in a post-quantum world.

Companies must make cybersecurity a business priority. **THEY MUST ASSIGN THE RESPONSIBILITY FOR TRACKING DEVELOPMENTS IN QUANTUM COMPUTING TO A TEAM,** led by a senior leader, such as the chief information officer or chief information security officer, that reports regularly to the board and top management.

+ **Identify priorities and create roadmaps.** Every company must map its years-to-quantum (Y2Q) risks by developing an inventory of connected assets, periodically evaluating the value of its data pools, and evaluating its exposure to new crypto standards. It must maintain a balance between the value of the data it has accumulated and the cost of protecting them, and develop a roadmap of its priorities.

+ **Plan, pilot, and test crypto agility.** Organisations must simulate Y2Q scenarios, such as the impact on their profit and loss, and develop countermeasures. They must conduct these exercises in coordination with their business units to ensure that the entire organisation has visibility into the challenge *ab initio*. In addition to developing pilots, executives must stress-test them to learn more about the problem, and gauge their crypto agility.

+ **Collaborate with rivals and the ecosystem.** Y2Q will not discriminate among companies, so leaders should adopt a collaborative approach to developing crypto agility, working with peers, and involving stakeholders such as academia, government, and digital start-ups. This approach will allow companies to share development costs; come to grips with the changing landscape faster; develop better Y2Q plans; and make credible policy recommendations. For example, in September 2021, 24 Japanese companies came together to form an industry council, Q Star, to understand, influence, and help businesses tackle the Y2Q problem.

The world is still some years away from a real advent in quantum computing, but when it arrives, it will be fast and it will be furious.

Just promise the world you won't get caught with your pants down. ✱

■ *Angela SP Yap is a multi-award-winning social entrepreneur, author, and financial columnist. She is Director and Founder of Akasaa, a boutique content development and consulting firm. An ex-strategist with Deloitte and former corporate banker, she has also worked in international development with the UNDP and as an elected governor for Amnesty International Malaysia. Angela holds a BSc (Hons) Economics.*

Fake News: Can You Handle It?

By Kannan Agarwal

Wrestling a US$78 billion problem.

Whilst the phrase 'fake news' has been bandied about since the late 19th century and was primarily used by news outlets to attack their rival, it was during former US President Donald Trump's tenure in office that its use entered mainstream lexicon; the term consistently trended on Google search from 2017 as one of the top searches and new organisations and alliances have been set up, such as the European Commission's (EC) High-level Group on Fake News and Online Disinformation, to counter the rise of mis/disinformation through digital channels.

Fake news are stories which contain no or just some verifiable facts, sources, or quotes. They could be propaganda (motivated to mislead readers) or designed as 'clickbait' (to generate clicks for economic profit). Author Claire Wardle together with Global Voices, a multilingual online platform for digital activists, have visualised the seven types of mis/disinformation campaigns (**Figure 1**) for readers to understand the landscape of fake news campaigns.

There are two kinds of fake news: those that are so preposterous you immediately know it's fake; and those that contain 'truthiness', the quality of seeming to be true and could, in fact, contain some factual elements to make it believable, but are overall inaccurate. The second category inflicts greater harm on society and the economy.

DOLLARS AND SENSE

One of the most comprehensive studies on the subject was conducted by economist Roberto Cavazos of the University of Baltimore. Commissioned in 2019 by CHEQ, an artificial intelligence (AI) and cybersecurity solution company, Cavazos' report,

There are two kinds of fake news: those that are so preposterous you immediately know it's fake; and those that contain 'truthiness', the quality of seeming to be true and could, in fact, **CONTAIN SOME FACTUAL ELEMENTS TO MAKE IT BELIEVABLE,** but are overall inaccurate. The second category inflicts greater harm on society and the economy.

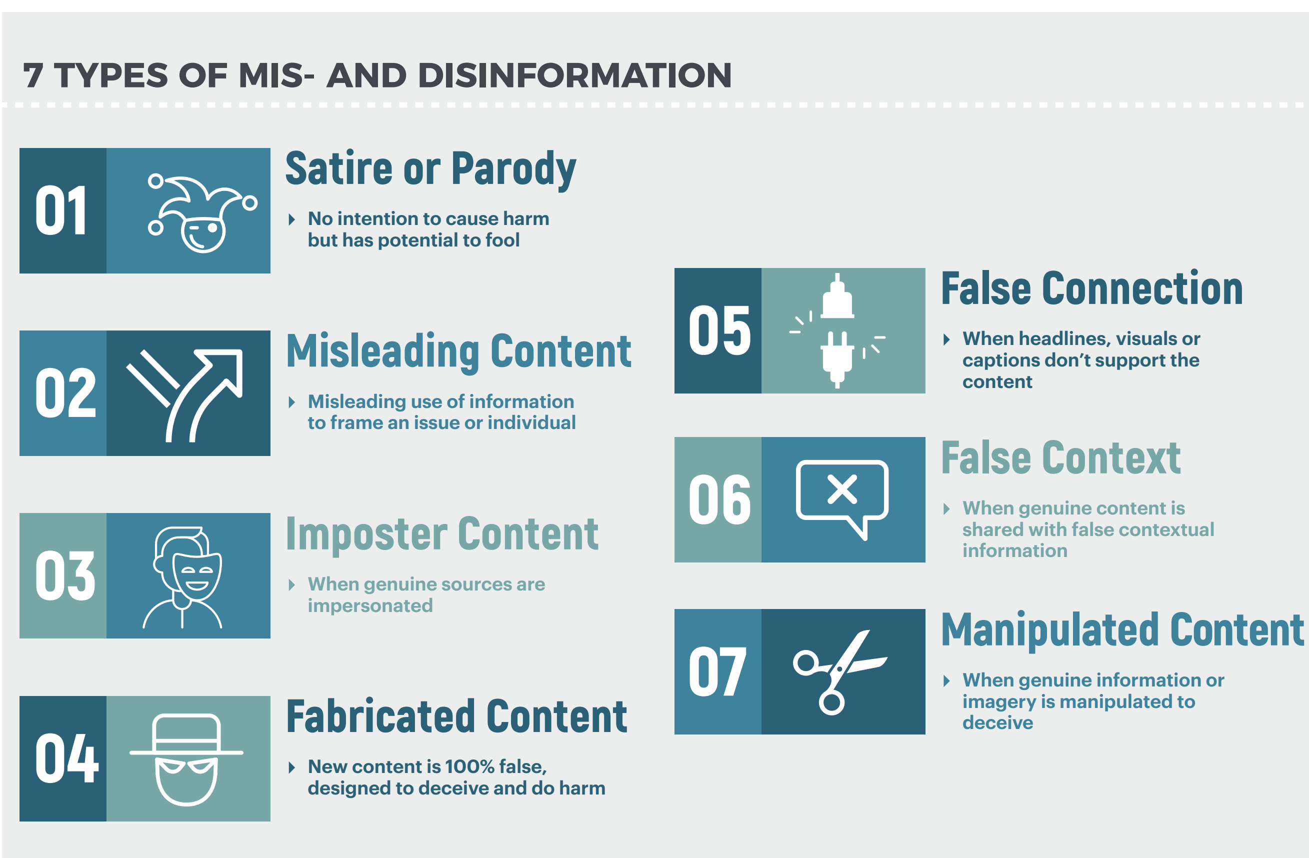


Figure 1: Seven Types of Mis- And Disinformation
Source: Claire Wardle and Global Voices, FirstDraftNews.org, *Fake News. It's Complicated.*

The Economic Cost of Bad Actors on the Internet, although using pre-Covid figures, remains one of the most in-depth global analysis of the economic impact of internet harm. The report measures the price paid by businesses and society across the range of online crimes, including 'pump and dump' schemes (where the price of a stock is boosted through false, exaggerated, or misleading positive statements), news of spoof trading (when a trader places a bid or offer with the intent to cancel before execution, thereby creating an untrue picture of actual demand for or supply of the security), and other sorts of financial disinformation or misinformation.

The report puts the total global economic loss at USD78 billion annually, which includes:

+ Stock market volatility caused by the spread of misleading messages online.
+ Difficulty in making important financial decisions, including those by pension funds, which in the US alone cost USD17 billion annually.
+ Reputation management and/or crisis management by brands to police and deny false information against their companies. To this end, the social media management/analytics market is estimated to grow to a USD9.54 billion industry by 2022.

"Fake news is further diminishing public trust in specific sectors — **TRUST IN THE NEWS MEDIA HAS DROPPED FROM 55% IN 2015 TO 32% IN 2019.** Trust in peer reviews has dropped (online reviews were found in the UK alone to influence USD26 billion a year of consumer spending each year). For instance, Tripadvisor claims 0.6% of its 66 million annual reviews are fake.

However, these are merely the direct financial costs – losses and opportunity costs imposed on society – that are being accounted for. According to Cavazos, indirect costs such as impact on the quality of life, increase in fear, changed behaviour, are less tangible but must also be priced in.

"Fake news is further diminishing public trust in specific sectors — trust in the news media has dropped from 55% in 2015 to 32% in 2019. Trust in peer reviews has dropped (online reviews were found in the UK alone to influence USD26 billion a year of consumer spending each year). For instance, Tripadvisor claims 0.6% of its 66 million annual reviews are fake. In 2018, 34,643 businesses out of the 8+ million locations listed on TripAdvisor received at least one 'ranking penalty' for encouraging or paying for the submitting of fake reviews."

"Other indirect costs include the effects of constant vigilance, energy and resources to defend against and repair damages caused by campaigns of misinformation. This effort is often diverted away from innovation, training, corporate social responsibility and many other vital economic sources of growth. These positive economic benefits, necessary for competition and growth, are casualties in the war against fake news."

STANDING UP

Although it is of global concern, very few solutions have been proffered on how corporations and brand owners can counter online dis/misinformation campaigns.

Organisations such as the European Commission's High-level Group on Fake News and Online Disinformation have remained just that – high level. Their report, *A Multi-dimensional Approach to Disinformation,* is of little practical use to brands and businesses that need

solutions and tools that work, now.

Think tanks are generally concerned with policy and legislation. Their recommendations focus on strengthening government oversight without infringing on freedom of expression, the role of news media outlets, and public responsibility to fact-check for responsible news sharing. What proactive measures can corporations take to protect themselves?

One of the most practical advice comes from public relations (PR) practitioner Kathleen Stansberry, an assistant professor of media analytics and strategic communication at Elon University. Specifically, her article, *The Financial Drain of Misinformation,* developed for the PR Society of America's Voices4Everyone initiative, advocates that organisations stop funding fake news by utilising the range of technological tools at hand.

For example, she cites JPMorgan Chase's policy of limiting online ad placements to only pre-approved websites, also known as 'whitelisting' or 'safe listing'. Another solution is for companies to invest in social listening, the process of observing and analysing digital conversations for red flags, and predict trending issues that could impact the brand.

It is important to note that although it is common for financial institutions to already have crisis communication teams who actively monitor social media, social listening involves predictive analysis and helps companies identify risks before they spiral out of control.

FAKE NEWS TO MATCH YOUR BUDGET

USD2,600
One social media account with over 300,000 followers.

USD55,000
Fund a Twitter attack to successfully discredit a journalist.

USD400,000
Influence policy changes on trade agreements, impact elections, or change the course of a referendum.

Figure 2: The Disinformation Campaign Menu
Source: Trend Micro, *Fake News and Cyber Propaganda: The Use and Abuse of Social Media.*

TICK TOCK

Financial markets have been dealing with fake news and hoaxes ever since money changed hands, but it was easier to detect crime in an analogue world. Today, digitalisation has expanded the surface of attack to include platforms and channels that are decentralised and at times, encrypted. Take, for instance, the forwarded WhatsApp message that sparked a run on the UK's Metro Bank in 2019 or similar online speculation in 2020 that saw at least five bank runs against small China lenders such as the Bank of Hengshui. Sent electronically, and sometimes using encrypted platforms, it is often difficult to trace the source of fake news.

"With technolog[ical] advances, and despite rapid efforts at detection," warns Cavazos, "the risks and costs of fake news will only grow. Fake-news-generated black swans may have the power to destroy iconic firms and generate untold economy-wide chaos and harm."

This bleak outlook means that banks must shore up their first line of defence, defined by the Bank for International Settlements as management and internal control functions which own and manage the banks' risks. In this instance, it means risk personnel in charge of digital detection tools, such as social listening and hoax-spotting algorithms, working together with the communications team. Vigilance is, in itself, a deterrent against hoaxers and hackers. ✱

■ *Kannan Agarwal is a content analyst and writer at Akasaa, a boutique content development and consulting firm.*

How Biodiversity Can Move the Dial on Climate Change

By Chartered Banker, UK

Approaches to integrate biodiversity into investment practices.

Loss of biodiversity is increasingly being seen as a systemic risk, with serious consequences for economic and social outcomes and as the next issue to be tackled along with climate change. There is a growing amount of global coordination, and numbers of bodies and frameworks coming together in order to quantify the impact of finance on biodiversity and identify how the sector can best make an impact.

But how important is a collaborative approach to tackling loss of biodiversity and what are some of the key partnerships driving it forward?

"The short answer is that global coordination is extremely important," says Tami Putri, Senior Principal Consultant, The Biodiversity Consultancy. "We're at an exciting time where we have seen true action, globally, from the financial sector at multiple levels.

"We're seeing governments commencing studies on understanding how nature is affecting countries' economies, and we're also seeing many financial organisations forming partnerships and groups voluntarily and setting themselves up to take action on nature. The most well-known is the Taskforce on Nature-related Financial Disclosures (TNFD), but there's also the Partnership for Biodiversity Accounting Financials and many others.

Anne-Marie Bor, Coordinator, Finance

For the financial sector, we've set up the Finance for Biodiversity Pledge and also **A FOUNDATION TO FACILITATE COLLABORATION WITH ITS SIGNATORIES.** A business perspective is now included in the draft Global Biodiversity Framework and also the alignment of private next to public financial flows is mentioned in the goals and targets.

for Biodiversity Pledge and Foundation, says the Convention on Biological Diversity is making significant inroads into the development of a global biodiversity framework.

"That's really a major piece of global coordination," she says. "For the financial sector, we've set up the Finance for Biodiversity Pledge and also a foundation to facilitate collaboration with its signatories. A business perspective is now included in the draft Global Biodiversity Framework and also the alignment of private next to public financial flows is mentioned in the goals and targets. As a foundation, we're accredited as an observer to the global biodiversity framework negotiations. We're advocating to have a more specific financial sector mention included and the associated guidance and regulatory frameworks, unlocking the unique financial services sector leveraging potential.

"I do think, though, that we all need to move faster on this. There's been a very severe decline of biodiversity due to climate change, but addressing biodiversity can be a major solution in the fight against climate change. Global coordination is needed to really shift the needle on this and to implement measures across the world within regulatory financial frameworks."

SUPPORTING THE SHIFT

For Bor, ensuring the financing of the protection of biodiversity comes down to having robust regulatory frameworks in place.

"This needs to be embedded in financial regulatory frameworks, to move beyond the voluntary actions that are currently being taken by individual institutions," she says.

"We cannot solve this crisis with just those individual, voluntary measures. We need regulation on assessing risks, on restoring biodiversity (also within ongoing investments) and on the conditions that support the sustainable transition to enable the shift we need to make as a society."

INNOVATIVE FINANCE

As international institutions come together to evaluate the most effective way of valuing biodiversity initiatives, the financial sector remains at the forefront of assessing the impact that humanity is having on nature – and how it can be turned around also by transforming finance activities.

"Just as is the role of the financial services in many things, the buck stops, essentially, with what financial institutions are doing," says Putri. "International financial institutions often require standards that are more stringent than national regulations, so I think the role of the financial sector is to ensure that robust due diligence and safeguarding is in place to stop the destruction of nature through the finances that it provides. This applies to many types of financing, from project finance to corporate loans.

"The second part of this is about greening finance, essentially moving finance away from sectors or activities that are disrupting nature. This is about how we are integrating nature into business models and exploring how considerations around nature shape origination strategies. This includes how we innovate in creating new business models that are centred around nature protection and restoration."

NO SILVER BULLET

There is growing demand from organisations, Bor says, for coordinated action, as well as a joined-up approach in how financial institutions engage with corporates.

"Corporates are receiving all kinds of questions from investors and it would be more effective if this were aligned with sustainable pathways within the sector and the move towards the positive impact possibilities that are there. Global coordinated action is about the reduction of negative impact, but at the same time it is also about enabling positive impact – not only amazing work through impact finance but also in enabling positive impact as part of engagement activities."

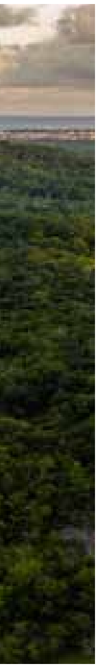
As awareness around the vital role that biodiversity plays in tackling global warming, new approaches are emerging to integrate biodiversity into investment practices.

"I think the key messaging here is that there's no silver bullet in terms of what the right approach is, and it's not one-size-fits-all," admits Putri. "We have seen approaches that work well and are mature, for example the applications of financial safeguards to project finance.

"Other emerging approaches we're seeing are portfolio-level impact and dependencies assessments. For example, there are now model-based approaches that enable financial institutions to perform a rapid assessment and understand their exposure to nature impact and dependencies by providing financial turnover data.

"One of the objectives of the TNFD is to shed light on how and under what

> The second part of this is about greening finance, essentially moving finance away from sectors or activities that are disrupting nature. This is about **HOW WE ARE INTEGRATING NATURE INTO BUSINESS MODELS AND EXPLORING HOW CONSIDERATIONS AROUND NATURE SHAPE ORIGINATION STRATEGIES.** This includes how we innovate in creating new business models that are centred around nature protection and restoration.
>
> **Tami Putri**
> Senior Principal Consultant,
> The Biodiversity Consultancy.



circumstances these measurement approaches work. The end goal is to be able to recommend a set of standardised processes as to how to understand the risks and impact on nature, how to manage it and then how to report or disclose the outcomes of it. It's really important that market participants now engage to test these emerging approaches and feedback the lessons learned to shape the future recommendations of the TNFD."

NATURE-POSITIVE IMPACT

For those working to direct funding towards the protection of nature, there have been developments at multiple levels over recent years, each creating new opportunities.

"One of the main developments I've seen with regard to investment practices is assessing impact at the portfolio level, through the use of footprinting tools, and knowing what your footprint is, as a financial institution. We recently published the second edition of a guide on these approaches, comparing them and providing detailed information on pressures covered and efforts associated," reflects Bor.

"The other field is engagement with corporates. We're noticing that our members are really keen to include biodiversity in their corporate engagement activities, but they're not set in stone yet. With a group of launching investors, we're looking into setting up a programme called Nature Action 100 to see how we can facilitate collaborative corporate engagement.

"A third area receiving more focus is innovation within the positive impact space. Aviva's Natural Capital Transition Global Equity Fund is a good example of this. It's a fund with a group of corporates included within it, but its function is to look into how to move those corporates towards a more nature-positive impact."

COMPLEX, YET POSSIBLE

As the financial sector and organisations across all industries reach a pivotal point in the move to protect biodiversity, the short-term priorities must lie in assessing the impact of the assets and projects being managed and funded.

"I think the main first step has to be around impact assessment and risk assessment, in order to gain a better understanding of the impact of current and future activities," says Bor. "I know carbon accounting is being increasingly implemented, but biodiversity impact assessment is the next step in there. It's more complex, but it must and can be done."

"This is just the beginning of the journey," adds Putri. "There is still a lot of homework for all of us to do, but I think the most significant progress that I've seen is the willingness to step up. It's quite amazing. In just a short period of time, we've seen almost every financial institution saying the same thing – that, in a global setting, they want to take biodiversity costs into account and play their part in addressing biodiversity loss.

"We feel that there is real work being carried out by financial institutions, especially in their goals to better understand their exposure to nature risks."

For Bor, the motivation from across the sector to make real change is not just a case of greenwashing.

She concludes: "I'm noticing more and more that the financial sector is sensing and reacting to the risks and the opportunities around protecting biodiversity that, in some instances, might have been expected from governments. It could very well be that the turning of the tide comes from the finance industry. I'm also noticing a high, intrinsic motivation from representatives from the sector to make sure this is going to happen. It's not just greenwashing." ✱

■ *This article previously appeared in the Chartered Banker magazine, UK, Autumn 2022 edition.*

I think the main first step has to be around impact assessment and risk assessment, in order to gain a better understanding of the impact of current and future activities. I know carbon accounting is being increasingly implemented, but **BIODIVERSITY IMPACT ASSESSMENT IS THE NEXT STEP IN THERE.** It's more complex, but it must and can be done.

Anne-Marie Bor
Coordinator, Finance for Biodiversity Pledge and Foundation,

REPO BY THE MINUTE

By Kannan Agarwal

A US$13 TRILLION MARKET IS SLOWLY GETTING TOKENISED.

On 17 June 2021, Goldman Sachs executed its first trade on JP Morgan's blockchain-based platform for repurchase agreements (repo), Onyx Digital Assets Network. Joining the Onyx-based repo syndicate enabled Goldman Sachs to trade repos with other third-parties within the network. The initial trade involved swapping a tokenised version of the US Treasury bond for JPM Coin, the digital coin developed by the bank and used for internal purposes, and took precisely three hours and five minutes lasting from origination, to trade, and the subsequent repurchase of the bond. In this instance, turnaround time is critical as the seller is charged interest by the minute.

As far as financial products go, the repo market is one of the slowest to evolve from manual voice-trading operations. Every day, between USD2 trillion and USD4 trillion repos change hands, allowing market participants to tap into low-cost secured financing for more efficient capital allocation. Institutional investors such as asset managers, money-market funds, and corporations with underutilised cash balances can also opt to invest their cash on a secured basis. Finally, central

banks use it as a monetary policy instrument by temporarily providing or removing liquidity from the financial system in order to promote stability and manage market expectations.

The 'electronification' of repo has its proponents and detractors in the market. On the one hand, these smart-contract repos solve some big issues that have plagued the financial sector, especially around counterparty risk. However, its use seems to best serve short-dated intraday repo trades for dealers, less so for money-market funds although financial institutions and fintech are testing its viability.

Securities advisory firm, Finadium, in its article, *Tokenised Repo for Cash Providers: Solving Settlement Problems,* reports: "…that the tokenisation of repo is a good idea, but current product designs are likely to inhibit cash provider adoption where it matters most: at money market funds and central counterparties. Making the leap from concept to reality for these firms means engaging with the legal and settlement mechanisms that have made repo into the successful USD13.4 trillion marketplace it is today. Without it, tokenisation may offer elegant solutions for dealers but may stall there."

RISK RECONNAISSANCE

Repos are short-term borrowings raised by dealers who sell their government securities to another party with the promise of a buyback at a slightly higher price, typically the next day, but as the Onyx repo platform proves, smart contracts by the minute are possible.

Although simple, the old-school repo process is fraught with challenges:

+ **Failure to deliver.** There are two points in time in which these could occur – at the beginning of a repo when the seller fails to deliver the collateral security (government or corporate bonds) to the buyer, or at the end when the buyer fails to deliver to the seller. In either case, it triggers a series of actions that need to be negotiated through consensus. If the parties had pre-agreed from onset of the contract to treat a failure to deliver the securities as a default, the buyer can declare that the seller is in default which triggers a series of actions. One action is a mini close-out, where the buyer exercises his right to terminate the failed transaction and the difference must be settled at the seller's cost. However, mini close-out mechanisms are expensive and, in practice, exercised only in extreme cases where the relationship between the seller and buyer breaks down. This is the reason why many brokers still rely on their mobile phones and strength of relationships to negotiate instead of transition to an electronic repo platform.

There are additional costs and risks. There is reputational harm to both the broker and the financial institution that fails to deliver. According to BNY Mellon, in the US, every day, roughly 2% of all Treasury and mortgage-backed securities set to change hands between buyers and sellers do not end up with their new owners by the time they are supposed to arrive. This could trigger millions of dollars in penalty fees daily for global financial markets. Buyers who never received the securities but had plans to enter this into their inventories will have to find late-in-the-day alternatives (e.g. borrow cash or other high-quality securities) to cover client activities, but last-minute borrowing comes at a premium.

+ **Counterparty risk.** Collaterals are rendered worthless if a default is called. Delays in delivering the security

Repos are **SHORT-TERM BORROWINGS RAISED BY DEALERS WHO SELL THEIR GOVERNMENT SECURITIES TO ANOTHER PARTY** with the promise of a buyback at a slightly higher price, typically the next day, but as the Onyx repo platform proves, smart contracts by the minute are possible.

In August 2022, Nyela Graham, a reporter for online financial technology news portal *WatersTechnology*, interviewed key personnel from JP Morgan for insight into the investment bank's blockchain-based Onyx Digital Asset network and its intraday repo solution, developed after years of research and development on blockchain use-cases. Below is an excerpt of the article, *Retooling Repo: How Broadridge, Bloomberg, Tradeweb, and JP Morgan Are Modernizing Repurchase Agreements.*

The bank was looking to identify use cases in which the then-fledgling technology could create new products or bring efficiency to existing ones. During those years of research, [Tyrone] Lobban, [head of blockchain launch and Onyx Digital Assets at JP Morgan] says the bank executed close to 100 proofs-of-concept, some of which included matching trades between brokers and custodians and corporate actions processing.

In 2017, attention shifted to the tokenisation of bonds by representing them on a blockchain. Through a partnership with the National Bank of Canada in 2018, JP Morgan issued a USD150 million, one-year floating-rate Yankee certificate of deposit using blockchain technology.

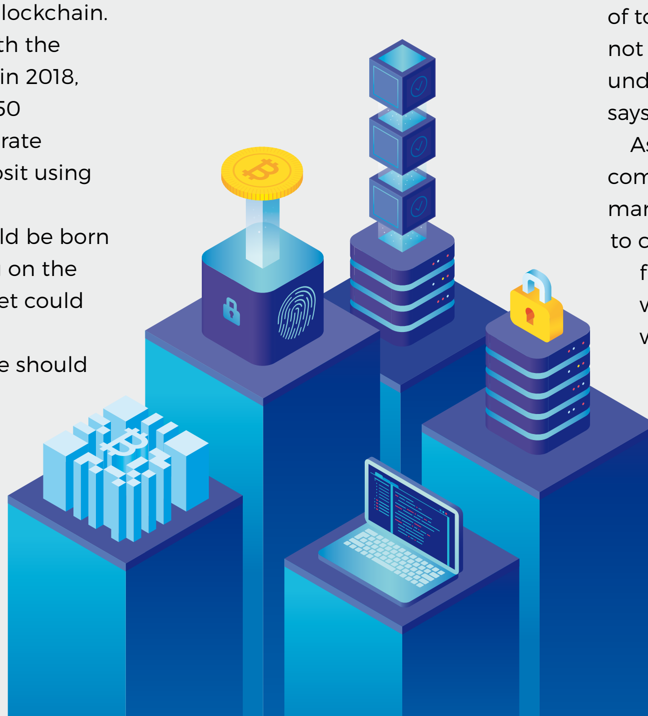
The Onyx platform would be born in October 2020, building on the idea that a traditional asset could be represented on-chain.

"The idea here is that we should be able to represent any type of traditional asset on-chain and start to use a blockchain for faster settlement, more transparency around that settlement, reducing fails processes, and having stronger guarantees around the delivery of assets in exchange for payments," Lobban says.

The intraday repo solution, launched two months after Onyx, allows JP Morgan clients to borrow funds intraday from the bank on a secured basis, while putting up collateral in the form of tokenised US treasuries.

"Because it's all happening on the same shared ledger, we can leverage things like smart contracts, and we can get much more precise about the length of time that our clients actually need to borrow these funds for," Lobban says. Instead of entering a repo transaction that has a standard overnight maturity, a client could theoretically borrow a billion dollars for three hours and return it before lunch.

In May, the bank launched the Tokenised Collateral Network on Onyx Digital Assets. Lobban says the work around the intraday repo solution led to a broader thesis around generally improving collateral and representing different types of assets on a blockchain.



"In the collateral markets, there's not just the challenge around the settlement timeframes alongside the need to move pieces of collateral, which you are looking to deploy in lots of different places, whether through tri-party agents or through different bilateral counterparties," says Thomas Pikett, vice president of Trading services product management at JP Morgan. "It's also about being able to make the maximum use of your asset pool available as collateral."

Like many firms and providers that embrace emerging technology, JP Morgan is aiming to create a service that clients can easily acclimate to. A representation of an asset should be as close to an asset as possible, with the accordant reference data, such as an ISIN (International Securities Identification Number), Pikett says. The record of ownership should be obvious and as easy to understand as a traditional asset.

"It's quite powerful in itself, because you can get the benefits of blockchain, you can get the benefits of tokenised assets, but you're not needing to rebuild systems to understand a new funky asset," he says.

As the more bespoke components of fixed-income markets have proved resistant to change, sources agree that a full overhaul of the existing workflows in the market is not welcome, nor possible. But if it's true that an efficient bond market is only as efficient as its repo market, then change is necessary and coming. Keeping familiar processes and frameworks in place may coax even the most reluctant of traders into the digital age.

could stem from temporary operational problems beyond the seller's control, such as infrastructure frictions, market illiquidity, and not necessarily credit issues. For as long as both parties agree the contract remains in force, the buyer can exercise his/her discretion to accept the delay and settle only upon successful delivery of the security collateral. This is a disadvantage to the seller who will still need to pay the interest on the repo even if he/she did not have access to the buyer's cash.

If defaults go above the normal daily threshold, this will lead to a crisis of confidence in the repo market. This recently occurred when the uncertainties of Covid-19 saw a spike in demand for US Treasury notes, resulting in an above-average number of settlement fails. The Federal Reserve stepped in to buy up the excess securities and counter threats to liquidity in the system.

+ **Collateral management.** This involves not just dealing with the features of the collateral (coupon, dividend, substitution addressing failures-to-deliver) throughout the term of the repo, but also accurately calling for variation margins whenever the collateral's value rises or falls in order to rebalance cash and collateral. Although organisations like the International Capital Market Association issue guidance on efficient variation margining, the ability to accurately call for variation margins depends on the skills, knowledge, and negotiation skills of the respective dealer, and allows financial institutions to optimise use of their collateral.

Repo tokenisation revolves around the concept of digitising and transferring the rights of the security or pool of securities. Essentially, the seller places its pool of securities in one custody account. **THE BLOCKCHAIN ADMINISTRATOR THEN ISSUES A TOKEN AGAINST THIS POOL OF SECURITIES** to the seller, which marks the start of a tokenised repo.

TECH'S QUICK FIX

How, then, does blockchain technology mitigate these risks?

Repo tokenisation revolves around the concept of digitising and transferring the rights of the security or pool of securities. Essentially, the seller places its pool of securities in one custody account. The blockchain administrator then issues a token against this pool of securities to the seller, which marks the start of a tokenised repo. Whoever is logged as the owner of this digital asset on the blockchain can freely transfer or trade this repo token 24/7 with finality, knowing that the underlying securities settlement will be done in accordance with the pre-set rules of the transfer. For repo buyers, they can bid on the entire token or proportional units of it, knowing that the underlying pool of securities is intact and transferable. Buyers will prefund a cash account that is held with and controlled by the blockchain operator, who maintains the ownership ledger. Once a deal is struck, the smart contracts running on a blockchain network make it possible for the settlement of both purchase and sale of the tokenised repo to occur simultaneously, similar to the physical delivery-versus-payment/receipt-versus-payment settlement methodology for the outright purchases of securities. ✱

■ *Kannan Agarwal is a content analyst and writer at Akasaa, a boutique content development and consulting firm.*

THE BUSINESS MODEL CANVAS: A STRATEGY TOOL FOR SUCCESS

By Derek Ariss

ITS SIMPLICITY AND EASE OF USE ALLOWS FOR A TRANSPARENT REVIEW OF ALL CORE BUSINESS COMPONENTS.

It's been said the world is changing faster and faster. So much change is happening these days in business that we need to review and refresh our business strategies repeatedly to survive. This means more strategy sessions at work and more business plans to be drafted and reviewed. Admittedly, I do a lot of business plan checking these days. It's not unusual to have a cup of coffee before I read a business plan for particular clients or organisations I work with.

In my experience, the business plan is often a 60-page-plus document. Usually, the document is thick, high on detail and strategic positioning, and low on application/implementation. Often the cup of coffee I started with turns into a pot of coffee. Eventually, I get to the point of matching the plan's detail with the implementation steps. All good; I appreciate that's the way things roll these days. But as some of you may be aware, I work in the innovation space as well as consult, and I have been thinking, "There has to be an easier, more transparent way of pulling together the business components for review, modification, discussion, and implementation!". I have found a better way. It is a strategic tool called the Business Model Canvas (BMC).

The BMC is a simple, powerful strategic template that lets business people identify the critical core components of a business and easily see how these components interact. What makes it easy to see?

Instead of the strategy being on tens of pages like a formal business plan, the BMC presents all the information on one page. Yes, the whole thing is on one page. The BMC format makes it practical to fill out and very easy to review all the core business component interactions. WOW.

By design, the top-down view of the BMC allows real-time collaboration between any group of participants. Participants fill out a template together and discuss issues as the document is completed. I find it curious that the BMC is taught in most MBA Classes and almost all entrepreneurship classes. Yet, the BMC is seldom used when it comes to day-to-day working environments.

This article aims to promote using the BMC as a simple and powerful strategic business tool.

In this article, I will:

+ Describe what a business model is;
+ Discuss the core components making up the BMC;
+ Highlight how to complete the BMC; and
+ Suggest further applications of the BMC in business.

Let's first be clear on what a business model is.

WHAT IS A BUSINESS MODEL?

For any business, a business model describes the rationale of how an organisation creates, delivers, and captures value. Value, believe it or not, is often but not always in the form of money.

Three parts make up a business model: They are (**Figure 1**):

- How the business creates value;
- How the business delivers value; and
- How the business captures value.

Once you understand how the business model works, you must also appreciate that business models change over time. Let's look at an example of how a grocery store used to operate 20 to 30 years ago. The grocery store created value by collecting all the produce and goods from farmers, butchers, and local manufacturers. Value was delivered to customers to visited the grocery store and bought the quantity they needed. Value was then captured in the form of cash exchanged at the cash register.

Today, the process may still be the same for the grocery store. However, new organisations like RedMart and HelloFresh are changing the way people get groceries and the way they eat. In turn, they are also changing the business model.

For example, when using RedMart, the customer uses an application (app) to order groceries online (value creation). Groceries are delivered to the customer's residence at a pre-arranged time (value delivery). Payment is made online (value capture).

To take the value creation process further forward, HelloFresh creates value by developing recipes for their customers and then delivering the produce for these recipes to the customer directly. The customers don't have to go shop for specific groceries or leave their homes. With HelloFresh, payment is made on their website via credit card using a subscription-based model. Notice how the business model for the grocery store has changed.

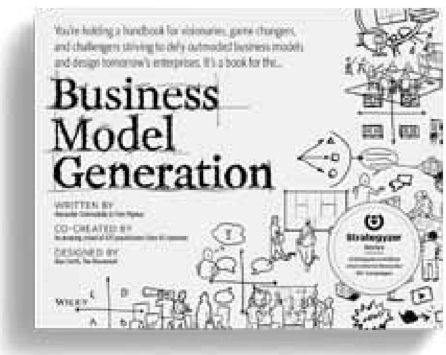
As technology has changed the playing field, many organisations have arisen due to their efforts to change their business models:

> Spotify changed the traditional music business model.
> Netflix changed the traditional audio-visual entertainment model.
> WeWork and JustCo changed the traditional commercial leasing business model
> Wise changed the traditional international payments business model.
> AliPay changed the traditional credit risk assessment business model.

Hence, understanding how business models work is becoming more and more relevant to strategy, business reviews, and innovation.

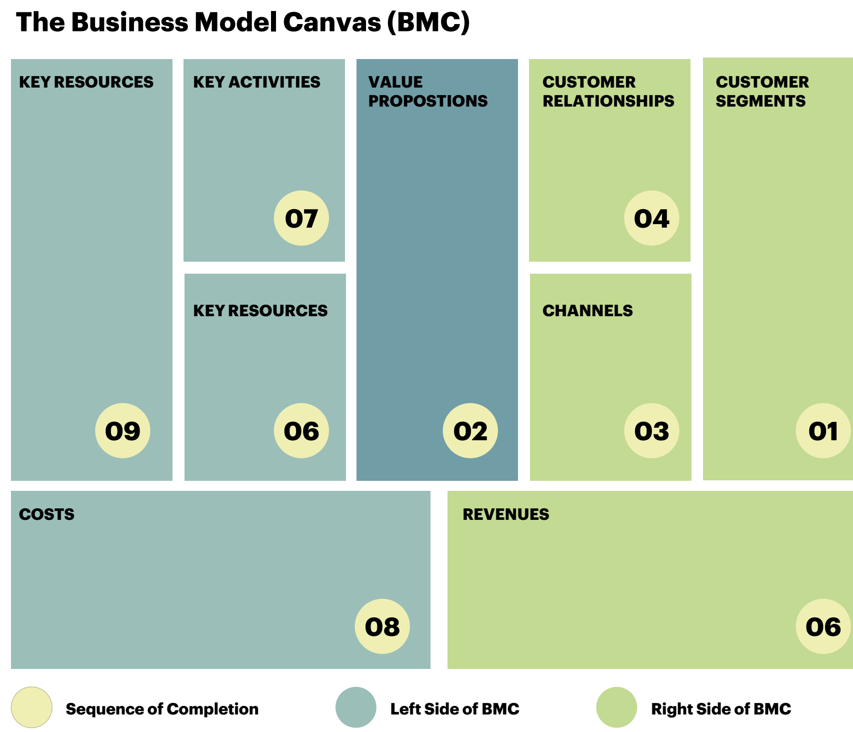
THE BACKGROUND ON BMC

In 2004, Alexander Osterwalder searched for a single definition of a business model. His academic paper entitled *The Business Model Ontology – A Proposition In A Design Science Approach* was concerned with looking at various business model definitions to create one that would work. It was from this research that the BMC arose. Thus, Osterwalder and Yves Pigneur wrote a book called *Business Model Generation* in 2010 in which the BMC was introduced.



SOURCE: John Wiley & Sons

FIGURE 2: BMC template.
SOURCE: Author



THE BMC

Similar to a Mind Map, where all the ideas of a concept are interconnected and put onto one page, the BMC does this when reviewing a business model. Everything you need to know is on one page, without flipping or referring to different components. This creates an accessible, easy-to-understand top-down view of the business.

HOW TO COMPLETE THE BMC

The easiest way to use and access the BMC is to download the free template from Osterwalder's Strategyzer website.

Once the template is downloaded, you will see that it is comprised of nine parts. All businesses are made up of these parts. Fill out the respective components with information you know about your business. This can be done as a group activity with a team or as an individual. Typically, the canvas is filled out with a group of peers because it allows for conversation and collaboration. When filling out the canvas template, the participants answer questions about each of the nine sections of the canvas on the BMC template and fill it out on the BMC (**Figure 2**).

The nine components of the BMC are:

1. Customer segments – who are your customers?
2. Value proposition – what value do you offer your customers?
3. Channels (delivery channels) – what channels do you use to deliver value to your customers?
4. Customer relationships – how do you interact with your customers?
5. Revenue streams – how do you generate revenue?
6. Key resources – what key resources do you need to run your business?
7. Key activities – what are the key activities of your business?
8. Key partnerships – who do you have strategic partnerships with?
9. Cost structure – what are your fundamental costs?

When completing the BMC, you look at these parts in detail.

For readers considering completing a BMC, included in the following table are key questions to ask (**Figure 3**).

As the information is completed, we see the business model for the business unfold.

To fill out the BMC, experience shows that completing the questions in the order listed in **Figure 3**: Key Questions works best.

To illustrate the best sequence to

FIGURE 1: The three parts of a business model.
SOURCE Author

complete the BMC, follow the numbers in **Figure 2**.

Following this sequence of filling out the BMC will feel like connecting the dots in a connect-the-dots game. At first, the dots look random. As you start connecting the dots, an image forms, and finally, when all the dots are connected, the image is crystal clear.

Similarly, when completing the canvas, you work through each of the nine business components in sequence. Once done, the entire image of your business model is clear.

TIP: By following this sequence, the right side of the BMC gets filled out first.

The right side of the BMC focuses on the customer or market. These factors include identifying your audience and distributing the product or service. Note the revenue stream is considered part of the right side of the BMC.

The left side of the BMC focuses on the business's internal factors, such as design, supplies, production, and costs, and gets filled out second.

Both sides of the BMC link with the value proposition in the middle, showing the value exchange between your business and your customers.

Overall, the nine business components are filled out and presented in this easy-to-see format. This makes reviewing your business model straightforward and clear.

Completing a BMC and strategy can be done collaboratively with a face-to-face group around a table physically or digitally on a white board. Either method works to allow meaningful discussion and thought between colleagues in about 45 to 60 minutes.

The most significant benefit of the BMC is the team application of the canvas to review, plan, and innovate your business strategy.

BMC APPLICATIONS AND MORE

Traditionally the BMC has been used for applications, such as:

- Reviewing existing business models;
- Developing new business models; and
- Analysing competitive business models to reposition your business.

	Business component	Key questions to ask
1	**Customer segments**	Who are you your most important customers? Who are you creating value for?
2	**Value proposition**	What value do you deliver to the customer? What are the problems you are solving for the customer? What bundles of products or services do you offer to your customer segments? What customer needs are you satisfying?
3	**Channels (delivery channels)**	How are you reaching your customer segments now? What are the best channels to reach your customers?
4	**Customer relationships**	How do you relate to your customer segment? What type of relationship does each of your customer segments expect you to establish and maintain? How are the relationships integrated into the rest of the model?
5	**Revenue streams**	For what value are your customers willing to pay for? What value are your customers presently paying for? How would your customers prefer to pay?
6	**Key resources**	What are the key resources needed for your value proposition/distribution channels/customer relationships/revenue streams to be created and maintained?
7	**Key activities**	What key activities of your value proposition/distribution channels/customer relationships/revenue streams are required?
8	**Key partnerships**	Who are your key partners? Who are your key suppliers? What key resources do you require from your key partners? What key activities do you need your key partners to perform?
9	**Cost structure**	What are the most important costs inherent in your business model? What are the most expensive key resources and key activities?

FIGURE 3
SOURCE: Author

However, I suggest this template be used for operational business reviews, especially around budgeting times. This permits teams to review all parts of their existing business models quickly, efficiently, and collaboratively.

With the BMC, everyone in the organisation can add to the strategic input of the business.

Bringing these factors together, from its simplicity and ease of use to its quick, transparent review of all core business components, you can understand why the BMC is a powerful strategic tool.

And yes, I like it more than most business planning tools because it delivers great results and saves me from drinking so much coffee. ✱

■ *Derek Ariss is Head of Innovation Education at Lightbulb Capital and is responsible for building the education practice, focusing on creativity, design thinking, technology, culture, and mindset conducive to innovation in finance. Derek also teaches part of the Singapore Management University (SMU) Certificate in FinTech and Innovation course and an Innovation Culture Catalyst course at SMU. He holds an MBA in International Marketing and Strategy and Bachelor of Commerce (Hons) from the University of Windsor, Canada, and a Bachelor of Science in Psychology and Biology.*

SO, HOW MUCH DO YOU MAKE?

By Majorie Giles

The debate on pay transparency continues.

Pay transparency is a policy in which corporations or employers furnish pay-related data to employees. This is increasingly being adopted – through legislation or voluntarily – as a means of tackling discriminatory pay practices by bringing down the barriers of secrecy and is considered by some as a tangible tool towards greater diversity and inclusion in corporations, especially for women in science and technology.

The United Nations' Sustainable Development Goals also advocates this as part of Goal 8.5, which aims "by 2030, to achieve full and productive employment and decent work for all women and men, including for young people and persons with disabilities, and equal pay for work of equal value".

It's important to note that each jurisdiction has had to find its own path, navigating the uniqueness of each ecosystem, and that the road to transparency can take many forms:

> In the US, 17 states currently have laws around pay transparency that allow employees to discuss their pay without fear of recrimination, but not all of these states require employers to provide salary ranges to job candidates. Some corporations voluntarily use pay-gap reporting as a strategy to prevent possible litigation, although some tech giants have recently been sued for alleged discriminatory pay practices when they did not sufficiently address pay disparities; these cases are still pending in the courts.

> In the UK, companies with more than 250 employees must publicly declare wage differentials based on either gender and/or race. The threshold for a similar law in Australia is 500 employees.

> In the EU, parliament voted this April that companies with at least 50 employees must be fully transparent about pay data. If there is a gender pay gap exceeding 2.5%, member states need to ensure these employers work with workers' representatives to conduct a joint pay assessment and develop a gender action plan.

> In Japan, effective July 2022, companies with more than 300 employees must disclose women's pay as a percentage of men's on their website and further distinguish between permanent and non-permanent employees.

> In Korea, since 2020, companies must report gender-disaggregated data on workforce characteristics and gender pay gap status, not pay gap data. The underlying causes of the pay gap must be studied and a gender action plan submitted to the government.

When it comes to talent management, studies have shown that opaque pay policies lead to higher turnover, with some employees more likely to leave within six months; whilst pay transparency increased employees' perception of fairness, trust, job satisfaction, and boosted individual performance. But it is far from a bed of roses.

DARK SIDE

There are nuances in the pay transparency debate which are rarely highlighted. Multiple studies confirm that making salaries transparent will

The numbers are in...

57%

who felt they were paid below market rate, were actually paid at or above market rate. Of employees who are paid above market

42%

believe they are paid below market. This means employees don't know whether they're being paid fairly.

Pay transparency assists in retaining talent. Employees who work for a very transparent organisation (classified as Level 5) are

65%

less likely to leave relative to an opaque organisation (Level 1). Also, employees who work for Level 1 organisations were

183%

more likely to leave relative to a Level 5 organisation.

Source: PayScale, 2021, *How Fair Pay Perception and Pay Transparency Combat Turnover.*

result in a drop in average compensation for employees across the board. In one instance, when the California state government published their city managers' pay scale back in 2010, average remuneration declined by 7% in 2012. Although transparency induces direct supervisors to streamline remuneration gaps quickly, the downside is that the same supervisors will be inundated with disputes by disgruntled staff and likely be solicited for non-financial rewards to offset the pay compression.

In *The Unintended Consequences of Pay Transparency,* published in the August 2022 issue of *Harvard Business Review,* authors Leon Lam, Bonnie Hayden Cheng, Peter Bamberger, and Man-Nok Wang state that the abovementioned dilemma can be avoided early on if corporates design their pay transparency programmes with three things in mind:

+ Make the performance-reward link clear and objective.

Companies will not reap the benefits of a transparent pay process if it lacks an objective performance measurement or reward system. Combining performance metrics that clearly link performance with rewards – for example, objectives, and key results – with continuous monitoring allows employees to better understand how their work relates to specific outcomes. This takes some of the pressure off managers to judge, often subjectively, individual employees' performance during appraisal periods, which is particularly relevant in jobs where performance is not easily quantified.

+ Provide training to facilitate pay-related communication.

One challenge in adopting pay transparency is the managers' limited understanding of their company's compensation policy, even though they are the ones managing employee inquiries. As a result, they fall short of adequately communicating the underlying processes of the compensation system. Connected to this is a lack of appropriate channels for employees to voice their feelings about transparency policy initiatives and a lack of resources for them to understand the pay system in the first place. Without proper manager training and learning resources for employees, a transparent compensation system will only lead to further confusion.

+ Restructure reward systems.

As the authors' research reveals that pay transparency fuels more non-monetary ideal requests, companies should consider formalising idiosyncratic deals (i-deals) into their reward structures, such as offering developmental i-deals to upskill employees and task or location i-deals to reward and retain loyal employees. When requests are not limited to an individual privilege or a hidden arrangement, the risk of unfairness can be mitigated.

MUZZLES OFF!

During the 2018 proxy season, impact-investing firm Arjuna Capital filed shareholder resolutions, calling on nine US-based financial institutions – Citibank, JP Morgan, Wells Fargo, Bank of America, Bank of New York Mellon, Amex, Mastercard, Reinsurance Group, Progressive Insurance – for detailed reports on the percentage pay gap between male and female employees across race and ethnicity, including base, bonus and equity compensation, policies to address that gap, the methodology used, and quantitative reduction targets. Two years earlier, Arjuna had successfully led proxy action against seven tech companies, including Adobe, Apple, and eBay to disclose their gender pay gaps.

In a surprising move, Citigroup stepped up and became the first bank in the world to voluntarily disclose its median gender pay gap and adjusted pay results ahead of the shareholder vote. The activist investment firm lauded the move and immediately withdrew its resolution.

In a January 2018 memo to its employees, Citigroup stated that on an

adjusted basis, its female and minority employees faced a pay gap of only 1% compared to male and non-minorities in the corporation. Several months later, it further disclosed that on an unadjusted pay basis, women and minorities at the banking group earned 29% less than men and non-minorities. Reactions were mixed. Some publicly panned the banking giant for the salary disparity, others lauded the group for its candour.

The bank took steps to raise the wages of female employees and set diversity targets within the corporation. It also championed pay equity in business through collaborations such as The Female Quotient, a thought leadership platform for women, to develop a free digital tool that provides companies with a snapshot of their raw pay gap for insights into what concrete measures should be taken to increase diversity efforts.

The bank took steps to **RAISE THE WAGES OF FEMALE EMPLOYEES AND SET DIVERSITY TARGETS WITHIN THE CORPORATION.** It also championed pay equity in business through collaborations such as The Female Quotient, a thought leadership platform for women, to develop a free digital tool that provides companies with a snapshot of their raw pay gap for insights into what concrete measures should be taken to increase diversity efforts.

Since then, Citigroup's 'raw' gender pay gap has slowly reduced, although it seems to have been sitting at 26% over the last two years. Globally, the share of women in roles from assistant vice president to managing director increased to 40.6% from 37% and the share of African American employees has also increased to 8.1% from 6%. Today, diversity goals are explicit targets on the scorecards used to assess managers' performance and the company is continuing to refine these metrics, including the implementation of a post-pandemic remote-work option that has helped to recruit and retain diverse talent.

The bank's 2022 memo states: "When we started on this journey in 2018, we were candid about our talent representation gaps among Black and women colleagues across the firm and we did something about it." The actual results are far from groundbreaking, but its moves have paved the way for other financial institutions to step up.

In the Asia Pacific, the momentum is fastest in Australia. According to the country's Workplace Gender Equality Agency (WGEA), the national pay gap is at 13.8% and the financial services sector leads with one of the largest gender pay gaps according to industry, reinforced by policies that enforce wage secrecy in employment contracts.

In March this year, Westpac was the country's first major bank to scrap age-old pay secrecy clauses in its contracts, allowing 40,000 employees to talk freely about how much they get paid without fear of recrimination. Its spokesperson said that the bank hoped the policy would contribute to broadening pay equity initiatives as it believed that "having open and transparent conversations and measuring that is what changes things." In less than 30 days, Commonwealth Bank Australia and other Australian banks followed suit.

A LAME-DUCK AGENDA?

This is just the beginning of reforms for pay transparency.

The International Labour Organization's (ILO) latest guidance, *Pay Transparency Legislation: Implications for Employers' and Workers' Organizations,* indicates that gender-responsive policies are coming back to the fore after several years of stalled progress due to Covid-19.

In its survey of employers' and workers' organisations in countries with pay transparency legislation, the ILO states that whilst there were pros and

HAPPENIN' DOWN UNDER

Australia's latest pay transparency policies and strategies require that employers with 500 or more employees must meet a set minimum standard to demonstrate their commitment to gender equality. Specifically, large employers are required to have a formal policy or strategy in at least one of the following areas:

- Workforce composition (gender equality in recruitment, retention, performance management, promotions, succession planning, training and development, and so on);
- Actions to achieve equal remuneration between women and men;
- Support for workers with family or caring responsibilities; and
- Sex-based harassment and discrimination.

The WGEA website offers resources on how to satisfy the reporting obligations, such as a salary calculator, reporting questionnaire, workplace profile, and so on. The agency also provides each relevant employer with a competitor analysis benchmark report on their gender equality performance, allowing the employer to realise which areas related to gender equality could be improved upon in their enterprise. The strength of Australia's pay transparency system is in the comparison of analysis benchmark reports, a mechanism to allow employers to compare their gender report to that of other enterprises in the same or similar industries, and other enterprises of the same or similar size.

According to information available through the WGEA, comparison of analysis benchmark reports encourages enterprises to act and address the results of their own analyses. In 2018, more than half of the enterprises that conducted a pay gap analysis and detected a pay gap reported their findings to the executive and board levels. Improved gender pay outcomes are far stronger for companies that combine specific pay equity actions, reinforcing the effectiveness of those actions with accountability through reporting to company executives and the board.

Source: ILO.

cons, the body of evidence tilts in favour of the former, which has net positive effects for the economy.

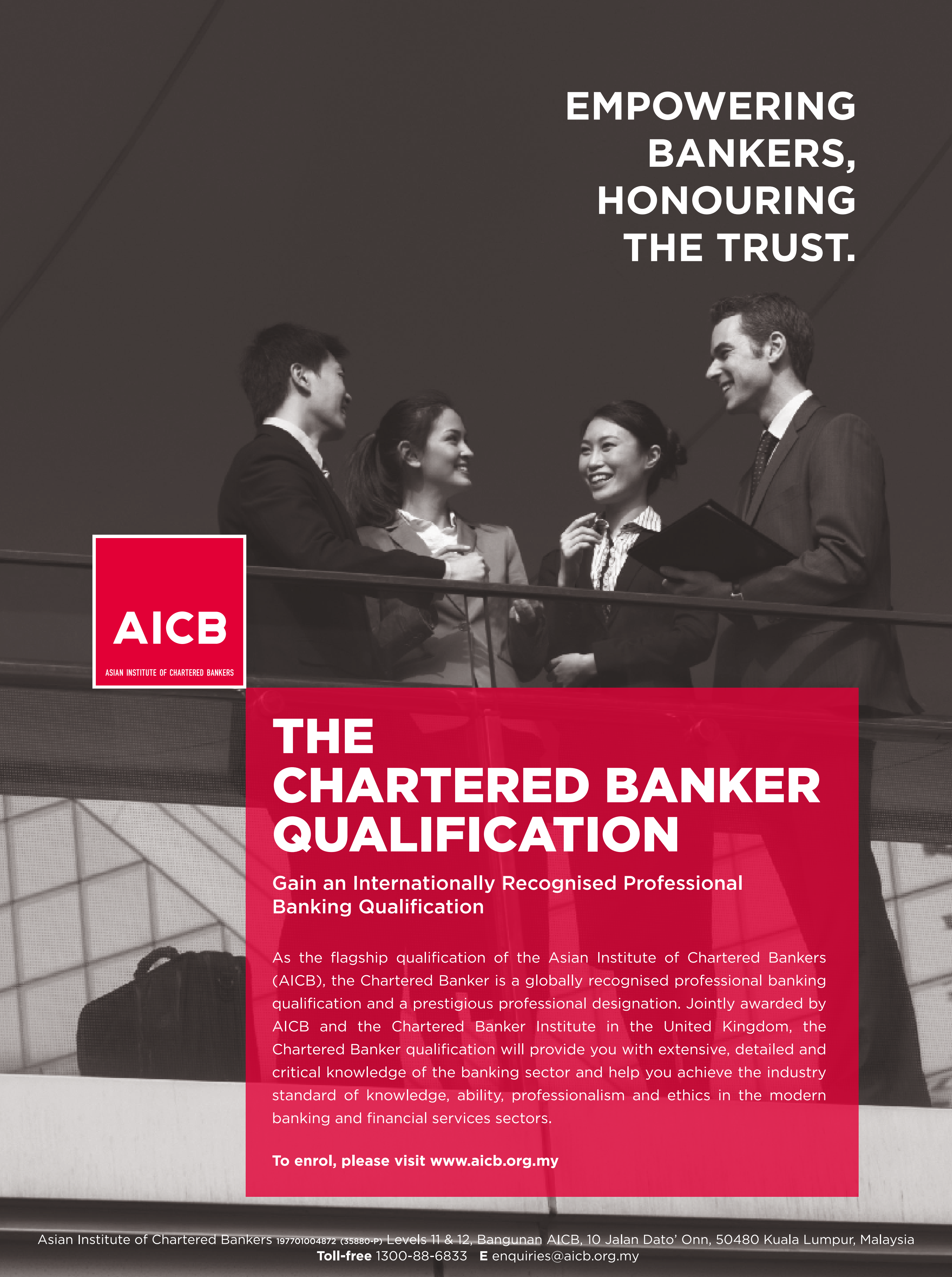
Current practices on pay transparency legislation can entail:

- Allowing employees to request and access information on pay levels in their enterprise;
- Requiring employers to disclose individual pay information to employees;
- Requiring employers to disclose an advertised position's salary to prospective employees, either during the interview process or in job advertisements;
- Prohibiting employers from requesting an employee's or prospective employee's salary history;
- Creating an independent body to provide employers with equal pay certification, if they meet certain requirements around gender-neutral pay;
- Obliging enterprises with a certain threshold level of employees (for example, 50) to publish information on gender and pay within their organisation;
- Carrying out regular audits on gender and pay in enterprises with a minimum threshold level of employees;
- Undertaking regular pay assessments in enterprises with the involvement of employee representatives; and
- Promoting the discussion of equal pay and pay audits during collective bargaining.

Almost all companies in Asia view this discussion with trepidation. As if to illustrate this point, whilst researching for this piece, I came across an online article on a leading news portal which touted "honest views" by CEOs on the Malaysian pay gap. Clicking on it led to…nowhere. A dead link.

Will this be the last we hear of it? ✱

■ *Marjorie Giles writes for Akasaa, a boutique content development and consulting firm, and holds a Masters in Clinical Psychology.*


EMPOWERING BANKERS, HONOURING THE TRUST.
AICB
ASIAN INSTITUTE OF CHARTERED BANKERS
THE CHARTERED BANKER QUALIFICATION
Gain an Internationally Recognised Professional Banking Qualification
As the flagship qualification of the Asian Institute of Chartered Bankers (AICB), the Chartered Banker is a globally recognised professional banking qualification and a prestigious professional designation. Jointly awarded by AICB and the Chartered Banker Institute in the United Kingdom, the Chartered Banker qualification will provide you with extensive, detailed and critical knowledge of the banking sector and help you achieve the industry standard of knowledge, ability, professionalism and ethics in the modern banking and financial services sectors.
To enrol, please visit www.aicb.org.my
Asian Institute of Chartered Bankers 197701004872 (35880-P) Levels 11 & 12, Bangunan AICB, 10 Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
Toll-free 1300-88-6833 E enquiries@aicb.org.my

Find out more at **www.aicb.org.my**