Grip.

SPRING 2023 / *Issue 1*

Connections

Managing the risk of network proliferation

globalRELAY PUBLICATION

GRIP magazine showcases the coverage that can be found on our digital information service, Global Relay Intelligence & Practice. It is aimed at decision makers working at enterprise corporations, financial services firms (especially banks, brokers, and asset managers), and in the insurance and commodities sectors.

It covers the interconnected relationship between Technology, Risk, and Compliance (TRC). It delivers insights on developing technology, key risks that need recognition, best practice, and the most effective methods to ensure compliance.

Global Relay has been providing compliance technology for more than 20 years. GRIP is an opportunity to showcase the deep subject matter expertise developed during this time. GRIP is made available in print and digital format to customers, prospects, and partners of Global Relay.

Grip.

Publisher
Alex Viall

Managing Editor
Martin Cloake

Editorial consultant
Richard Cree

Designer
Nikki Ackerman

Sub-editor
Rachel Horner

Cover artwork
Tonya Golmant

Contributors
Jennie Clarke
Carmen Cracknell
Andrew Davies
Ben Edwards
Bob Hawk
Chip Jones
Alex Viall

Printing
Geoff Neal Group

Issue
01

MIX
Paper from responsible sources
FSC® C013204
FSC www.fsc.org

This publication has been printed by the Geoff Neal Group on sustainable, FSC®-certified paper made from trees from well-managed forests and other controlled sources. All coatings used in the making of this magazine are water-based. All inks used in the making of this magazine are vegetable-sourced. Geoff Neal Group recycles the chemicals it uses in this process and also any waste that is a result of the production process.

"Measuring how intelligently we handle change, as well as how we gather intelligence about the results of change, is becoming increasingly important"

Einstein said "the measure of intelligence is the ability to change". Measuring how intelligently we handle change, as well as how we gather intelligence about the results of change, is becoming increasingly important to the regulatory and compliance community.

Arguably one of the greatest changes we are coming to terms with is the change in how we communicate. We live in a more connected world. Means of communication are easier to use than ever, and this contributes to a blurring of the boundaries between the professional and the personal. And the 'always on' culture makes it harder for us all to keep our guard up. All of this matters when compliance and regulation have to be considered.

Our cover feature focuses on connectors and why they are vital to our efforts to help process information in the rapidly changing environment caused by platform proliferation. We also examine the unintended consequences of regulatory change in the UK car insurance market, reflect on long overdue changes to Rule 17a-4, and ask how much change there really is in the UK government's Edinburgh Reforms package.

The unfolding Wirecard case could also lead to changes in the way economic hot prospects are judged, especially in light of subsequent events at FTX. We consider the fallout from the courtroom as the trial continues. Plus we have interviews with lawyer Tim Dolan and KPMG partner Aaron Stowell.

You will also have noticed another change — the name of this magazine. After two years as *Orbit TRC*, our print offering has been rebranded as GRIP magazine, to tie in with our new digital information service Global Relay Information & Practice (GRIP). There is more about that over the page, and we hope that you will continue to enjoy our analysis of relevant issues, however we present it.

Change, it is also said, is as good as a rest.

Martin Cloake
Managing Editor

Contents

Grip. magazine

GRIP magazine is a showcase for the information you can find every business day on Global Relay's new digital service, Global Relay Intelligence & Practice (GRIP). The service is designed to help practitioners in regulated industries gain the practical insights needed to make informed decisions in a shifting compliance landscape. You can find it at grip.globalrelay.com

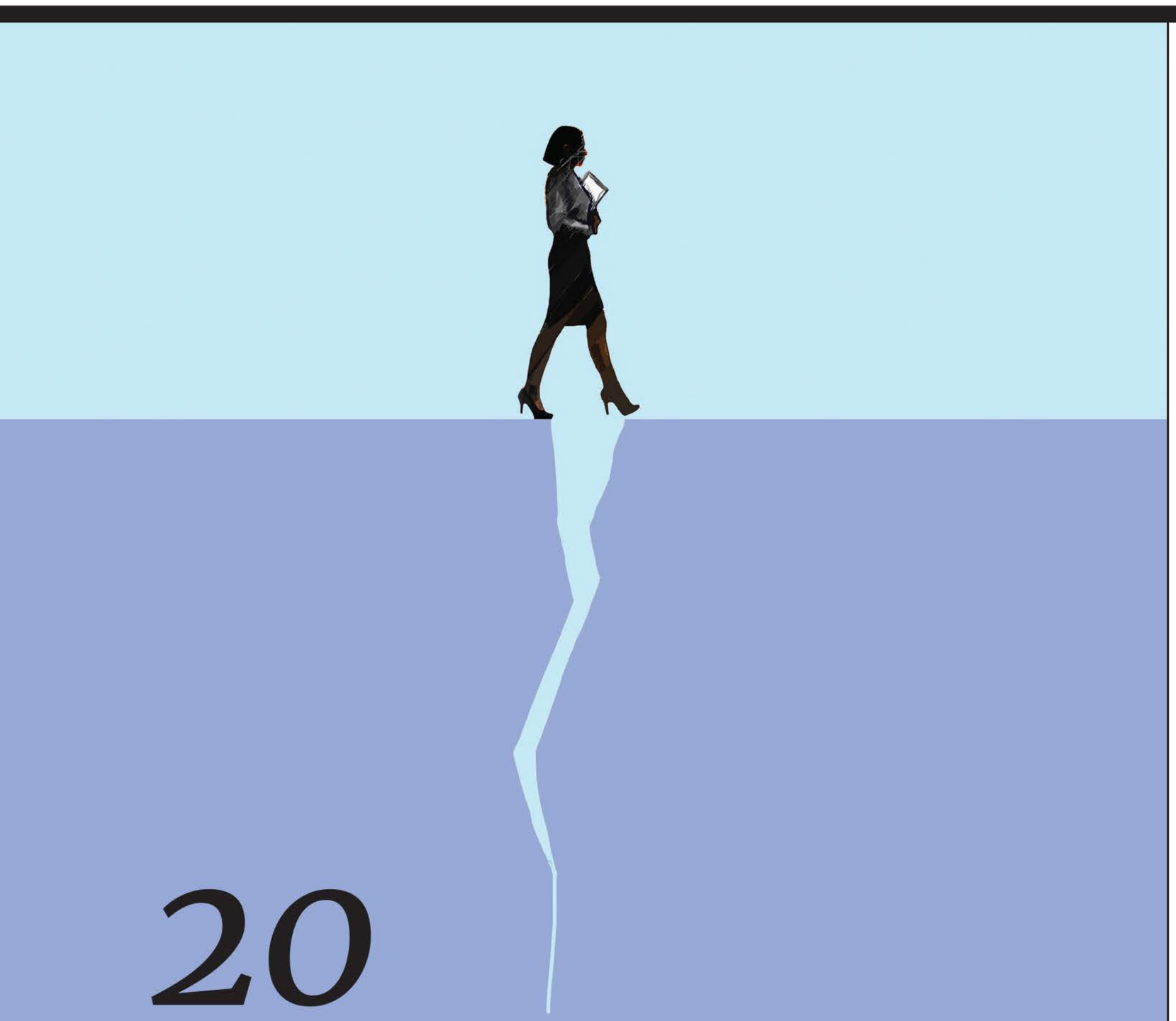
We decided to launch a digital service after the successful reception given to *Orbit TRC* magazine two years ago. It was a natural progression to create a website that would build on this and offer greater breadth of coverage and an opportunity to engage.

To align our print and digital offerings, *Orbit TRC* has become GRIP magazine. Published three times a year, it will feature original material alongside selected stories from the website. We will use it as a physical calling card to demonstrate the quality and range of coverage we provide.

GRIP provides digestible, practical content that focuses on regulatory and operational developments in key markets. Our coverage is presented in five pillars — compliance; data; ESG; regulation and technology. Material is provided by a full-time global team of experienced business journalists working alongside subject matter experts, and supplanted by regular comment and opinion from credible practitioners in the field.

We are pro-regulation and pro-enterprise, and we are committed to covering the widest range of news stories and viewpoints — fairly, independently, and accurately. We won't be breaking much news, instead we will offer insight and analysis on developments in regulation and compliance and on fintech industry trends, together with practical information to allow compliance and operational teams to do their job with confidence and knowledge.

We hope you enjoy the magazine enough to visit the website and sign up.



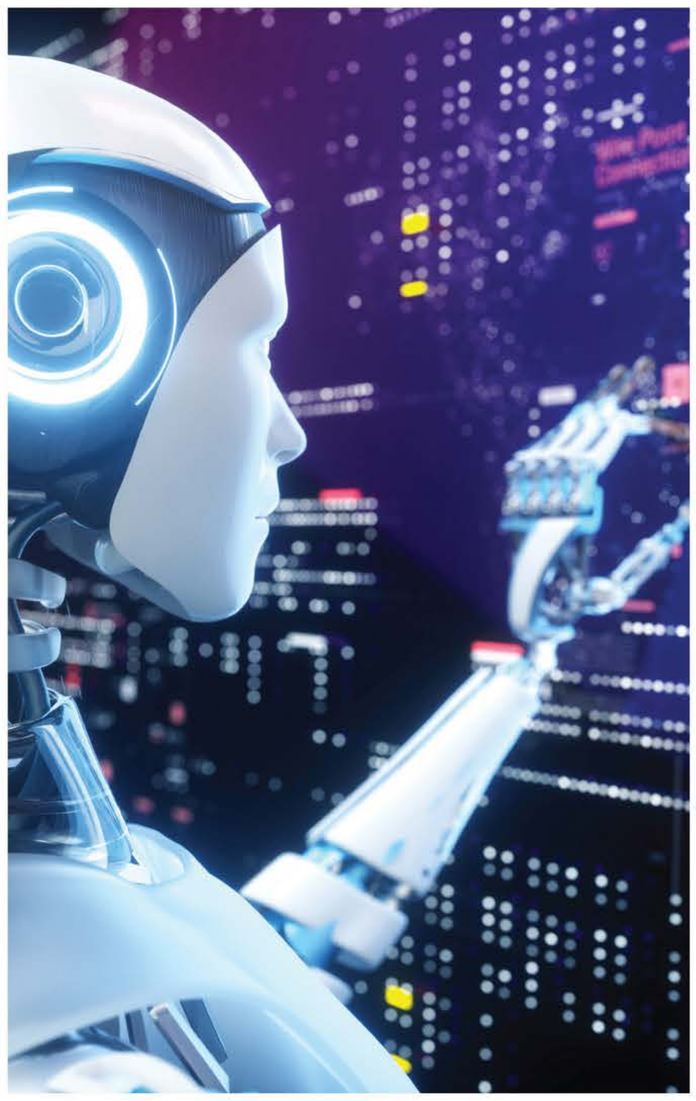
20

Interview

Tim Dolan

We spoke to the regulatory lawyer about bridging the gap between aspiration and implementation as the UK faces a period of significant change

IN PRACTICE



DEFENSE IN DEPTH

Industry conferences tackle pressing issues

Our director of regulatory intelligence picks out the trends and key takeaways for staff in banks, brokers and asset managers, after attending legal and compliance conferences in Amsterdam, London and Surrey

Words by
ALEX VIALL

AFME AMSTERDAM
OCTOBER 2022
LEONARDO ROYAL HOTEL, AMSTERDAM

The conference odyssey began in Amsterdam at The Association for Financial Markets in Europe's (AFME) Annual European Compliance and Legal event. It was well attended and it was evident people were excited to be able to meet face-to-face again and share advice on current regulatory change and practice. Delegates were senior compliance and operational personnel.

A particularly engaging panel included Jacqueline Joyston-Bechal, MD, JP Morgan; Seung Earm, Head of Regulatory & Territory Office, BNP Paribas; and Guillaume Loeuille, CCO, Global Financial Services, Natixis.

The panel agreed that while compliance had traditionally been more of an advisory function, and resourced by lawyers for the most part, it had more recently become a risk management function. The combination of conduct risk, operational risk and compliance risk is a recognition of the fact that the role of compliance, whether providing expertise or navigating regulatory change, is viewed through the lens of risk identification and how to assess it. It is a risk-based approach. Not everything can be covered and there is a need to prioritize. There is a lot to manage, but a framework that can process operational risk and compliance helps.

Day-to-day risks require prompt attention, but with less resource available, as departments are under cost pressures, prioritization is crucial. It is essential to identify the key risks attached to the kind of business sought. The compliance framework has evolved significantly in terms of where legal risk and conduct might occur, how the three lines operate and the nature of the tasks in each line.

What keeps compliance officers awake at night?

The volume of regulations is overwhelming. No one can honestly claim to have full coverage and compliance. How do firms deal with all this regulatory change and manage risks when all are expected to do more with less? EU and UK divergence is a further challenge, as new regulations emanate from both and many firms with offices in the UK are required to comply with both. They can be quite different, and this can be operationally burdensome to follow and implement on time. It makes it an uneven playing field for those that have to comply with both regimes.

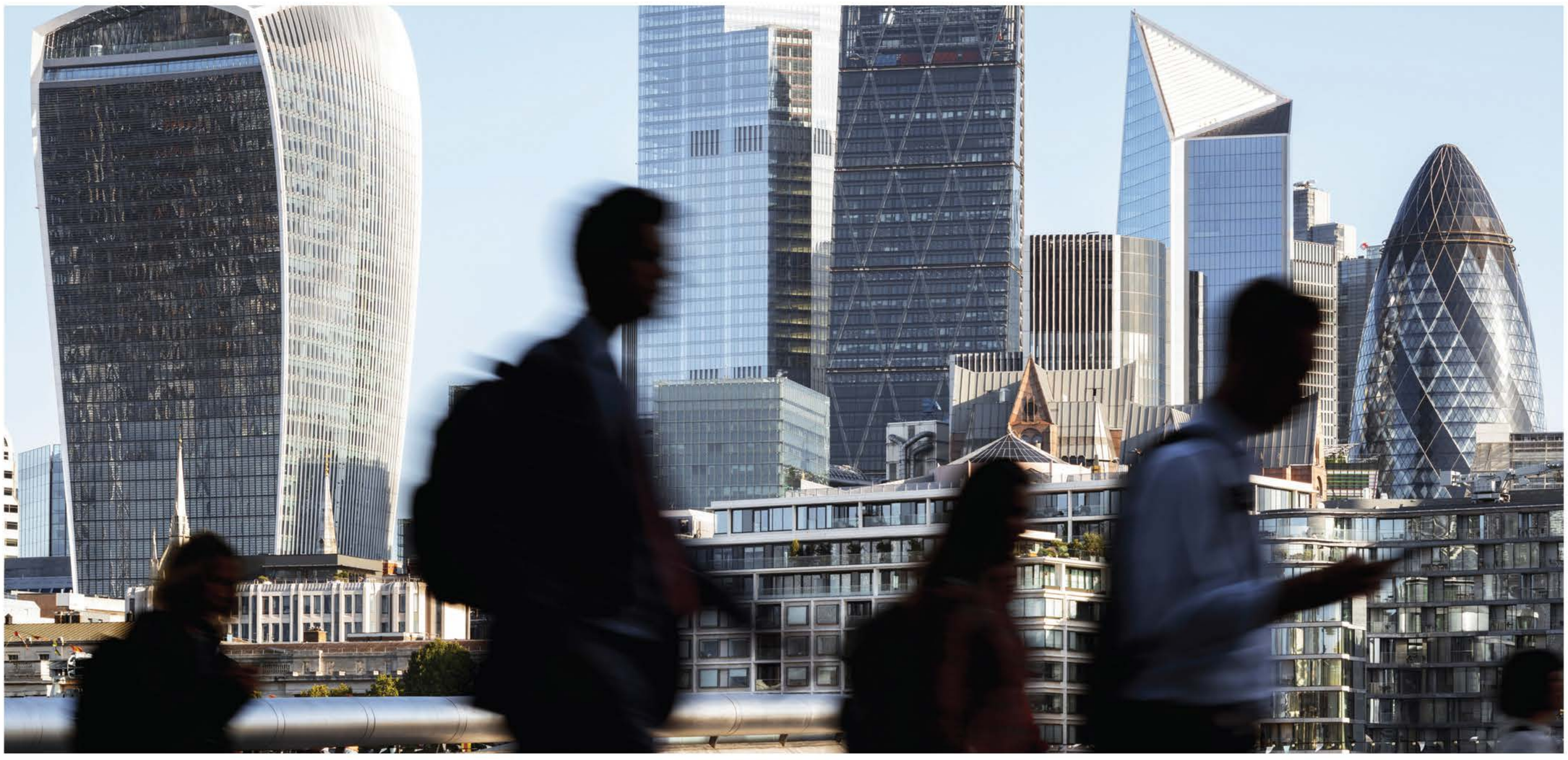
Data and its quality is also a big concern, alongside the increased reliance on information technology. It needs constant investment and updating to ensure systems are compatible. Ultimately a robust framework is needed so all of this is working. Controls and monitoring, as well as risk management, are so important for multi-function responsibility.

Monitoring is not a new concern, but most are still struggling to get it right.

Finally, the need to focus on consumer duty and what is a proportionate approach for wholesale firms and the risk of indirect retail interactions that must be right. This is a concern when faced with a principles-based regulatory regime.

Compliance process around financial crime and market abuse needs to move away from false positive reduction to quality time on effectiveness. The balance is not breaking things while upskilling and embracing new challenges. Much of it depends on finding the right people.

Financial crime is usually the top risk for any financial institution. However impressive your controls, the risk is always there as it is so complex, whether you are looking at sanctions, KYC or AML. Most senior management and boards can cope with risks if they have been reported, discussed and mitigated.



XLOD LONDON: THE FUTURE OF NON-FINANCIAL RISK AND CONTROL ACROSS THE THREE LINES OF DEFENCE

NOVEMBER 2022

LONDON

This event was part of the regular series hosted by XLOD in London and New York. It included a packed program and was well attended by surveillance and compliance professionals, as well as vendors.

Particularly enlightening was a keynote from Jamie Bell, Head of Secondary Markets Oversight at the UK Financial Conduct Authority (FCA). He tackled the most noteworthy enforcements the FCA published on market abuse in 2022. And he warned the audience of compliance, legal and audit personnel that there were more of these in the pipeline.

One of the most revealing comments he made was that the FCA regarded the gap between good firms and average firms as being too wide. He qualified this by stating that surveillance capability was not keeping pace with new requirements and natural change.

The fines the regulator levies are always uncomfortable, but they are powerful agents for change. Risk surveillance must stay aligned with the risks inherent in the business. This forces everyone to make the right, albeit costly, investment decisions.

He warned firms that the regulator wanted every firm to be respectful of the required standards — no one gets a free ride. It is essential to keep markets clean.

He moved to more positive topics and stressed that the FCA preferred to work with firms to improve standards. The regulator views its plans for risk surveillance as a shared goal across the industry. Market abuse risk assessment (MARA) is at the heart of this.

The FCA does not specify how to conduct a MARA, but it will challenge one if it is not clear in its approach, lacks granularity and is not comprehensive. It must also be updated periodically. The regulator, said Bell, appreciates this is an expensive process.

There is always a trade-off between cost and risk. Only the firm can manage that, and it depends on the risk appetite. The FCA has an axiom, which is that a regulated firm can outsource a capability but not the risk.

Bell warned firms to avoid a "boiling the frog moment" where the environment they are in changes around them almost imperceptibly. Without knowing it, the temperature has risen to a lethal level. This is comparable to market stress.

Seven market events have taken place recently (October 2021-22) where the indicative prices have exceeded 15 standard deviations.

This has a huge correlation to existing systems that have not been refined or calibrated to these extraordinarily different market conditions. Imagine a system last set five years ago? A lack of attention to this is going to be very challenging to justify to the FCA. »

HFM LEGAL EUROPE
NOVEMBER 2022
PENNYHILL PARK, SURREY

This gathering of compliance and legal heads from a diverse group of hedge funds based in London took place in the comfortable confines of Pennyhill Park in Surrey. It was a select group who clearly knew each other well and the debates were frank and of high value.

Topics covered included ESG Frameworks and Investor Expectations. It was clear that the debate related to how labeling funds (Article 6, 8 or 9) is one of the most crucial distinctions in these early stages. When asked if fund classification under SFDR matters, 50% said it did and Article 8 is the one; 44% disagreed and said it did not matter, while 6% said it did and Article 9 was the way forward.

There also seemed to be much more focus on what firms, analysts and investors mean and consider relevant for the 'E' of Environmental, Social and Governance. The imperative is to look at the environmental impact your own business has, as well as what climate change will do to companies in which you invest, and their supply chain and production process. The scrutiny of 'S' has receded with the new distractions of war in Ukraine and global inflation concerns. It is also much harder to measure than carbon emissions.

There was an ominous warning about the perils of green bleaching — where a firm promotes green credentials and is subsequently exposed after analysts, critics, consumers or competitors shoot holes through the claims. The best advice given by one person on the panel was to "say what you do, do what you say, and document all of it".

A panel on the risks related to geopolitics and the challenges of cyber started inevitably with the impact of Russia's invasion of Ukraine.

This caused a flurry of compliance activity related to sanctions around the KYC piece of actual fund investors, and then the origination of investments and investee companies (further complicated if derivatives were involved).

One of the panellists said it was now evident that any form of passporting from the UK into the EU was never going to be possible post-Brexit; this has meant that the UK FCA has become more important than ever in terms of its regulatory approach and the impact on those it regulates. It will be fascinating to see how the FCA gets on and if this or subsequent governments reform the regulatory structure to account for this significant change. The European Securities and Markets Authority is on the rise and the UK FCA needs to establish its place and identity.

The panel all agreed there had been an explosion in cyber activity from state-sponsored actors. More resources are needed each year to account for this general increase in threat. Thought is required to imagine challenging issues such as no access to the office, loss of power, trading systems hacked. There is never enough resource for this — it can become a bottomless pit — but the key is to focus on protecting the core.

Regulatory expectation here grows all the time. But the target is moving as those instigating these threats are extremely smart. The CBI's operational resilience guide was recommended for its prescriptive detail and focus on mapping and analysis.

If an employer specifies the need for five days a week in the office the candidate pool drops

75%

A popular session covered recruiting and retaining top talent, with a look at the workplace and its challenges post-pandemic. Harry Rogers, a specialist recruiter, set the scene, describing what attracts candidates right now. Remote work is still appealing, especially to more junior personnel who have only been working since the pandemic. Three days remote, two in the office is common. If an employer specifies five days in the office, the candidate pool drops 75%. The more senior the role, the less this applies. One of the panel said she and most of her team were "TWaTs" — always in on Tuesday, Wednesday and Thursday.

What keeps people loyal to a firm?

In many cases, it's about trust in colleagues. Recognition and empowerment go a long way. Respect from others and knowing your team are looking out for you is important. Interesting work and recognition for the value you bring has an impact. Backing from the business through a decent budget is of value.

Feeling fulfilled and flexibility post-pandemic are also appreciated. Having access to senior management and also having a senior management that was honest and trustworthy were deemed the non-negotiables in choosing and remaining with an employer.

The panel concluded that personal development opportunity, excellent communication, and honesty and trust from managers were the things most likely to help retain talent. ●

Hedge funds bemoan lack of clarity

In the UK in early December we sat down for a lively, albeit chilly, Hedge Fund Roundtable. With a bursting agenda, a few topics were consistently revisited throughout the hour-long session. A running thread was the lack of regulatory clarity for fast-approaching compliance deadlines

Words by
JENNIE CLARKE

Consumer Duty

Hot on the heels of the HFM Legal event, the confusion surrounding the applicability of the new Consumer Duty persists.

The FCA's Sheldon Mills recently acknowledged that the regulator "had not been great at explaining" the new duty and its benefits, an assessment many agreed with. In particular, questions have arisen around how far the duty will apply to, for instance, firms that reference a retail class in their prospectus even where it's an offshore fund.

Another sticking point is the appointment of the Consumer Duty Champion, with most uncertainty as to who is suitably independent of the existing product and governance sphere. The idea of appointing a non-exec director was floated by some.

There have been degrees of clarity, but questions remain in advance of the July implementation deadline.

WhatsApp and off-channel comms

US regulators have continued to issue fines to firms for off-channel unrecorded communications.

The main question seems to be around degrees of investigation; how far down the rabbit hole must you go to show compliance. It was generally agreed that it isn't sufficient to just tell people not to use, for example, WhatsApp, but there is no consensus about how far you must go to show that employees are adhering with any policy set down.

Some prefer lexicon searches for WhatsApp — and having frank discussions with staff who are found to say things like "let's discuss on WhatsApp". Others choose to look at phone records to deduce who is talking to whom — asking more questions where communications don't add up or the dialogue suddenly goes dead.

The consensus appeared to endorse fear tactics and educating staff about the dangers of getting caught.

Making senior leadership adhere to compliant communication rules is also a concern, especially where personal phones are involved.

At the moment, it appears to be a high priority for SEC and FINRA, though whether FCA may soon take a similar approach was up for debate.

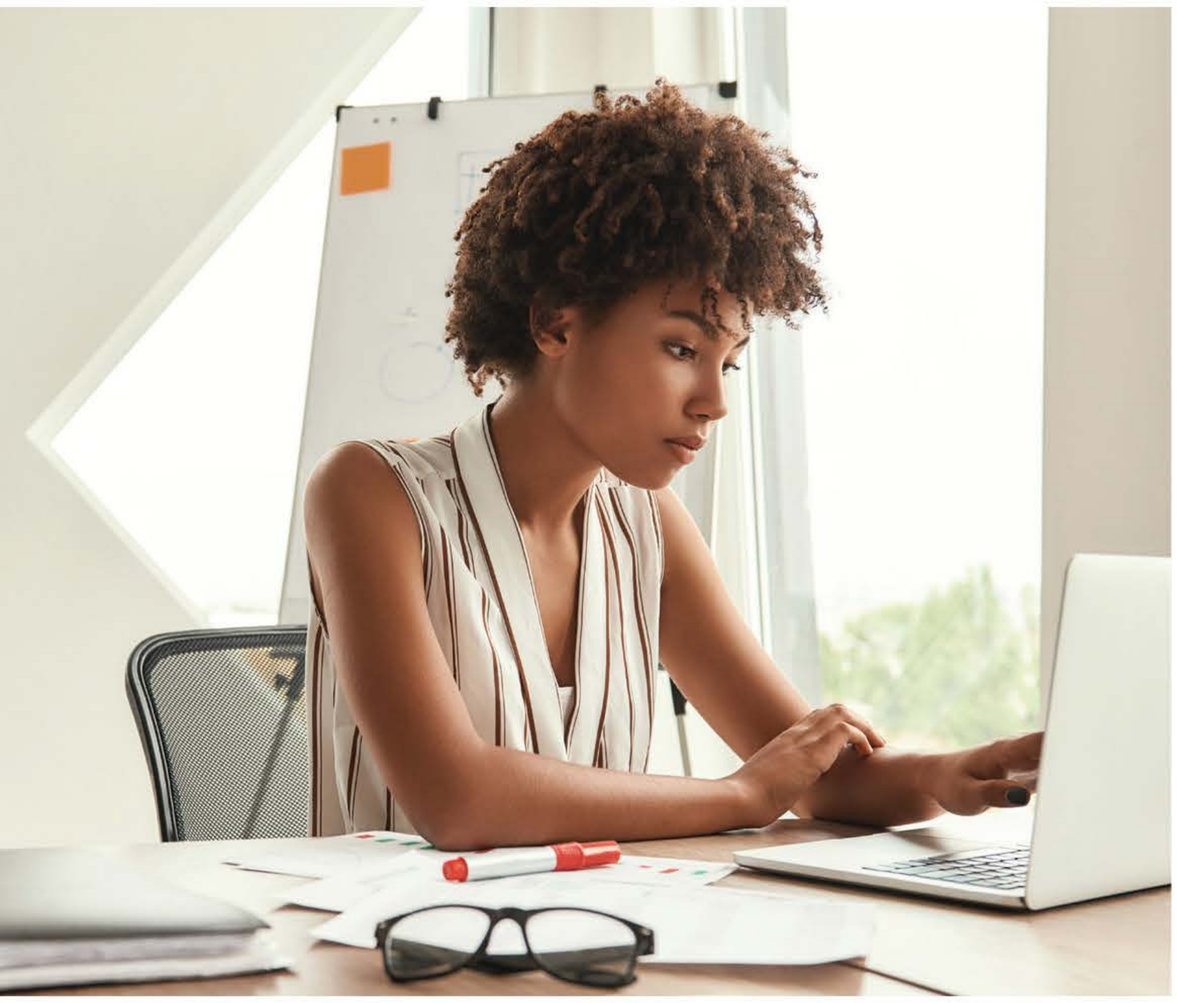
SEC's new Marketing Rule

There were varying degrees of frustration with the SEC's new Marketing Rule, with those that market their products heavily finding the change to be onerous, at best. Some of the group actively use LinkedIn, Twitter and other mediums to market their offering to a wider audience, and are now grappling with SEC compliance, as well as renewed stringency from the DoJ.

Some in the room were ERAs, but are treating themselves as RIAs to avoid any missteps with the new rule. The key appears to be to establish clear guidelines, revise existing marketing to apply, and meet those guidelines moving forward. It also appears to mean a lot of updating and a lot of internal discussion.

Hiring and retention

On a practical level, and out of the hands of financial regulators, is the issue of recruitment and retention. Most agreed that it was difficult to find new compliance staff in a post-Covid economy. Most junior employees are looking to work from home, which isn't deliverable or effective within a global compliance team. If remote working is not available, the pool of talent is significantly reduced. ●



Testing times for all firms with EXAMS

Both the SEC and FINRA issue reports for broker-dealers and investment advisers. Firms would be wise to pay heed

By **CHIP JONES**, *Executive Vice-President, Global Relay*

The Securities and Exchange Commission's (SEC) Division of Examinations (EXAMS) released its annual Examinations Priority Report in February — it can be found on the SEC website. US broker-dealers (BDs) pair the content of the report with that of the Financial Industry Regulatory Authority (FINRA) Exam and Risk Monitoring Report to review current compliance practices and WSPs to focus compliance resources for the year. Investment advisers (IAs) focus primarily on the report for annual compliance planning, as IAs are not regulated by FINRA. The report is extremely helpful for compliance professionals as it serves as a guide for the year and an instrument to assist in the justification for compliance resources.

I applaud EXAMS for continuing to be honest and transparent regarding the large regulatory gap that exists between IAs and BDs. When 50% of BDs are examined annually versus just 15% of IAs, there is a serious problem. It is also troubling that EXAMS still has a list of IA firms that have yet to be examined.

To be clear, the SEC is not at fault here. Its lack of resources to conduct IA exams falls squarely on Congress. The regulatory gap between BDs and IAs demonstrates the value of a self-regulatory organization model. BDs bear a higher level of regulatory scrutiny because FINRA is not reliant upon Congress for taxpayer dollars to oversee the broker-dealer community.

> *"Kudos to the SEC and FINRA for continuing to provide this invaluable guidance"*

Areas of interest

I won't summarize the entire 40-page report, but I will highlight a few areas of particular interest. IAs can expect a strong focus on the implementation of the SEC's Marketing Rule. Given that 206(4)-1 has not been substantially amended in more than 60 years, the SEC will want to ensure that "RIAs have adopted and implemented written policies and procedures that are reasonably designed to prevent violations by the advisers and their supervised persons of the Marketing Rule". The SEC Marketing Rule can be found on the SEC website.

Approximately 35% of IAs manage private funds. A private fund is basically a mutual fund that does not solicit investors from the general public. With the dramatic increase in private fund assets over the past several years, EXAMS is wisely focusing on this area.

A perennial favorite of both EXAMS and FINRA is Reg BI and Form CRS. EXAMS will be looking at IAs from a fiduciary standard perspective and BDs from a Reg BI perspective, ensuring that investors' interests always come first.

Both IAs and BDs have a requirement to deliver Form CRS. EXAMS will be looking to ensure that the form is accurate, delivered in a timely manner and that the most recent version is posted on a firm's website.

Cyber scrutiny

Both IAs and BDs can expect to be scrutinized with respect to information security and cybersecurity. Cybersecurity risks will only continue to increase and therefore firms must be extremely diligent to ensure that records are secure and critical systems are protected.

EXAMS will also focus on the "security and integrity" of third-party vendors. Data security is of primary concern to Global Relay, including SOC 2 audits annually and ISO 27001 certification. It's no surprise that EXAMS specifically highlighted, for both IAs and BDs, that it would be focusing on policies and procedures for "retaining and monitoring electronic communications".

Given the SEC's recent enforcement activity in this area, firms should obviously ensure that all Ts are crossed and Is are dotted when it comes to electronic communications supervision. Global Relay is the industry-leading expert in electronic communications capture and supervision.

I firmly believe that the SEC's and FINRA's reports are essential tools for compliance professionals with both IAs and BDs. Informed compliance professionals from both industries read these reports closely and use the guidance provided to plan for the year. Kudos to the SEC and FINRA for continuing to provide this invaluable guidance. ●

IMAGE: ADOBE STOCK

Russia sanctions: low impact makes the case for more action

One year into a new regime of sanctions against Russia and the impact has been disappointing. But, says Andrew Davies, this is merely a sign we need to take further action

By **ANDREW DAVIES**, *Global Head of Regulatory Affairs, ComplyAdvantage*

The scale and level of coordination with which measures against Russia were implemented was unprecedented. There can be no doubt that they have affected Russia's financial strength, both overall and its banking industry in particular. Estimates of the impact on Russia's GDP in 2022 range from a contraction of 2.2% to 3.9%. However, it can't be ignored that the combination of national and individual sanctions has not crippled military funding, nor has it delivered a fatal blow to Russian president Vladimir Putin's aggressive tactics.

Historical efficacy

While the oldest recorded example of economic sanctions took place in ancient Greece, they have become an important first-response mechanism in modern international politics as a way to counter aggression, terrorism and human rights abuses. But increasingly people around the world are asking: do they actually achieve what they set out to do or are they merely a paper tiger, more menacing in print than in reality? Aren't the subjects of economic measures able to easily hide their activities, remaining relatively unscathed? And, lastly, how can they be effective if some countries refuse to enforce them, as has been the case now with India and China?

The answer is a complicated one. If you compare the financial and regulatory landscape of 2022 with that of 1992 (during the Gulf War and the start of the Balkan War) or even that of 2002 (following the 9/11 attack in the US and the conflicts in Afghanistan and Iraq), technology has transformed the implementation of sanctions, making them more difficult to evade. Financial services companies that support sanctions enforcement are now able — and expected — to update and reflect newly named individuals or organizations instantly, eliminating the time lag that only decades ago was easily exploited.

Another positive is that technology has also helped economic sanctions evolve from a blunt force instrument (which historically hurt civilians with hyperinflation and deprivation) to become a surgeon's scalpel that can be focused on the politicians and business leaders supporting corrupt regimes.

However, there remain two unfortunate realities: there will always be non-aligned countries which choose to ignore the will of the international community; and sanctioned individuals still can, and do, operate, moving money undetected in the financial system by working through shell companies or associates who have not been flagged.

International cohesion

This is why it is imperative for governments and regulatory agencies to make an honest assessment of Russian sanctions and use the learnings to make much-needed improvements to the system. While there is nothing that can be done to force the international community to act as a united front, there are other weaknesses that can and should be shored up.

> *"Technology has helped sanctions evolve from a blunt force instrument that hurt civilians, to a surgeon's scalpel focused on politicians"*

There needs to be far more international collaboration involving intelligence agencies, regulatory bodies and financial institutions. For sanctions to be effective, they need to be immediate.

For them to be immediate, the companies that are on the hook to implement them need to know they are flagging the correct person. Intelligence agencies need to share their broader array of data on these individuals to eliminate the false positives that cause delays.

Next, the related data needs to be used to create a more layered approach to sanctions screening that includes family members, known associates and businesses, and other related information.

With this additional data, the full network comes to light, making it possible for behavioral analytics to identify patterns of transactions, detecting and choking off funding to the sanctioned person or organization.

Finally, politically exposed persons need to be identified and risk assessed on all relationships on an ongoing basis. Currently, governments do not provide a singular source of truth with regards to who is appointed or elected to public functions at national or local level. This requires labor- and time-intensive manual research.

Providing this information regularly would improve the timeliness and efficacy of sanctions and would have the additional benefit of strengthening the detection and prevention of financial crimes, such as bribery and corruption. ●

Connections:
managing the risk of network proliferation

It is 19 years since Facebook launched. Twitter followed a few years later. LinkedIn has been available since 2003, but took time to develop beyond a niche business resume service. Social networking was in our lives but was, during its infancy, understated.

Now, according to digital consultancy Kepios' January 2023 data report, 59.4% of the population of the planet uses social networking platforms regularly. That's 4.76 billion people. And the number of users is growing at an annualized rate of 3%. All of which means the way we interact with each other, including the way we do business, has changed completely.

Words:
MARTIN CLOAKE & ALEX VIALL
Illustrations:
TONYA GOLMANT

The 15 biggest social media platforms

- *Facebook has **2.958 billion** monthly active users*
- *YouTube's potential advertising reach is **2.514 billion***
- *WhatsApp has at least **2 billion** monthly active users*
- *Instagram has **2 billion** monthly active users*
- *WeChat has **1.309 billion** monthly active users*
- *TikTok ads can potentially reach **1.051 billion** adults over the age of 18 each month*
- *Facebook Messenger's potential advertising reach is **931 million***
- *Douyin has **715 million** monthly active users*
- *Telegram has **700 million** monthly active users*
- *Snapchat's potential advertising reach is **635 million***
- *Kuaishou has **626 million** monthly active users*
- *Sina Weibo has **584 million** monthly active users*
- *QQ has **574 million** monthly active users.*
- *Twitter's potential advertising reach is roughly **556 million***

*Pinterest has **445 million** monthly active users*

SOURCE: KEPIOS

The decision to adopt new technology or new methods of working is often made without a proper analysis of the compliance risk. This is especially true of activities or technologies that were not created with financial services users in mind.

Social media was not originally designed to satisfy financial regulators' compliance requirements and, consequently, might offer only a snapshot of a user's data at any particular moment. Someone's data may include messages, recipients, posts, and the status of the system at a point in time. But the picture could still be incomplete from an audit-trail perspective, because someone could post something and then delete it quickly without a record of that activity being captured.

Wake up and smell the risk

Market research from GWI, and quoted by Kepios, reveals that "the typical social media user actively uses or visits an average of 7.2 different social platforms each month, and spends an average of more than than two-and-half hours per day using social media". That suggests, according to Kepios, that people spend roughly 15% of their waking lives using social media.

In short, it's hard, if not impossible, to function nowadays without using a social media platform. And harder still to do business without having an active presence on more than one.

The scale of reach, combined with ease of use, has contributed to a blurring of the lines between personal and professional. We looked at the compliance issues arising from just one platform — WhatsApp — in the last issue of this magazine.

There is also an important distinction between social and enterprise collaboration. Social is designed for community outreach and these platforms offer business-to-consumer communication (for example LinkedIn, Facebook and Twitter). Pure business-to-business enterprise communication takes place through providers such as Bloomberg, Refinitiv and IceChat, where regulatory concerns are a higher priority.

As easy-to-use channels of communication proliferate, it becomes less practical to control the use of pre-approved channels for business. It's human nature to take the easiest route or be led by the customer's channel of choice. Cue the critical role of connectors.

Typical users visit 7.2 different social platforms a month, and spend more than 2.5 hours a day on social media

Early adopters

One of the first connectors to be developed by Global Relay came from Bloomberg in 2003. It was a plain text converter. Since then, Global Relay and Bloomberg have collaborated to conquer truncated email addresses, data gaps, malformed messages, duplicate messages, anomaly events, and numerous other areas.

Global Relay worked to identify many of the problems that Bloomberg faced, testing its fixes and patches on behalf of its customers and then reimporting data to »

ensure complete integrity of the data set. It also put in extra effort to reprocess malformed data.

Enterprise XML connectors were the market standard until a few years ago, when application programming interface (API) connectors became the norm. This development has moved in lockstep with the proliferation of enterprise messaging tools and the amount of choice has increased the risk for users.

If you want to minimize the chances of business communication being non-compliant, you have to go to where people are communicating. This means having the ability to pipeline any comms from any original source into an environment where that data can be stored, monitored and retrieved.

For customers, there has to be total trust in the data plumbing (from source to archive vendor to processing and back to customer) so that there are no leaks or blockages that will threaten the data set's regulatory integrity.

The role of data processing

The only way to validate this is to examine the data processing and enforce the key components of reconciliation and connectivity, so that nothing is missed. Customers need reports, validation and verification to ensure that all data is captured. This is the best way to certificate completeness.

Think about the scale of this task. There are six social media platforms with more than one billion monthly users each worldwide, and the top 15 platforms (see box) have more than 400 million users each. LinkedIn, which doesn't publish monthly user data and so is not included in this list, has 849.6 million users. Add in other heavily used comms channels such as Slack, Microsoft Teams, Bloomberg Messenger, Zoom, Symphony, AT&T … and the list goes on.

Each time someone uses an app such as Facebook, or sends an instant message, or checks the weather on their phone, an API is used. But it is not unusual for the newest messaging platforms to have no API at all.

Executives should thoroughly analyze a communication platform before it is approved for use. As an example, some platforms may have compliance APIs but only log a subset of the communication. This poses a risk to the user and the institution that not all of an individual's activity will be logged, archived and retrievable.

Not all enterprise users need this level of audit integrity, but almost all financial services companies do. The delta is represented by what is missing from a regulatory requirements perspective — compliance teams can advise on whether communications can be captured to satisfy the regulators. This risk needs to be balanced against any reward in terms of new customers and revenue from using a communication platform, and whether it is sustainable.

As these platforms add new features to appeal to their end users, their compliance solutions tend to fall behind while they prioritize supporting the new features, which can result in data gaps.

59.4%
of the world's population — 4.76bn people — use social networks

This is growing 3% a year

Will it go to penalties?

The vast amount of data and the increase in channels through which it is transmitted is not insignificant, but with penalties for absent recordkeeping now so high, no organization can afford to take any short cuts when it comes to archiving data and ensuring it is searchable in the most efficient manner.

"Apart from not losing any messages, one of the major challenges comes when we have to interpret the granularity and complexity of the data from the service provider," says Sunny Chind, Group Product Manager at Global Relay, who works within the team focused solely on connectors. "What we have to investigate is how to bring the best out of the data and subsequently furnish it so it provides extra value to the customer."

"Enrichment" is the term Chind uses to describe the process. "It's about ensuring we provide pertinent information that is meaningful through business logic, about removing redundant information, structuring the data, breaking down the data into 'conversation-sized' pieces that can be turned into an email for archiving purposes," he says.

Enriching the information enables users to know where to look for the valuable nuggets, and that's where having knowledge of the financial terrain combined with technical expertise helps to gain a real competitive advantage.

"We enrich the data to drive efficiency for compliance officers in their searches, monitoring (to identify anomalies) and management via the archive," says Chind. "It's about highlighting the edits on what has changed, grouping related events into a single email record, enriching for analytical reports within the archive, and ensuring consistent formatting across connectors so that horizontal searches and monitoring can be seamlessly observed across multiple datatypes, thereby ensuring a good user experience.

"There is a lot of information which is ingested. Connectors provide an efficient and rapidly expanding

"We have to investigate how to bring the best out of the data and subsequently furnish it so it brings extra value to the customer"

conduit to further finesse the data which is gained from the service provider and then sent to the archive with consistent formatting, so that it can be subsequently parsed, indexed and analyzed in order to provide a collective view of the regulated archive data. Our mantra, of ensuring that what we capture is encrypted at rest and in transit, is always implicit as part of the connectors ecosystem."

The voice challenge

The challenges are going to increase further as the use of voice messaging and spoken word content grows exponentially. While there is still industry debate on how valuable voice will be in a compliance environment, owing to the complexities of correctly transcribing speech patterns, it would be a mistake to assume that voice is not going to grow as a channel that people use with increasing ease and in increasingly complex ways.

"In relation to voice, we are now offering customers the option of transcribing their regulated user voice media content which is embedded inline within the email body sent to the archive. This provides the 'value add' in allowing reviewers to look at policy flagged hits of the transcribed message, thereby saving time and money," says Chind.

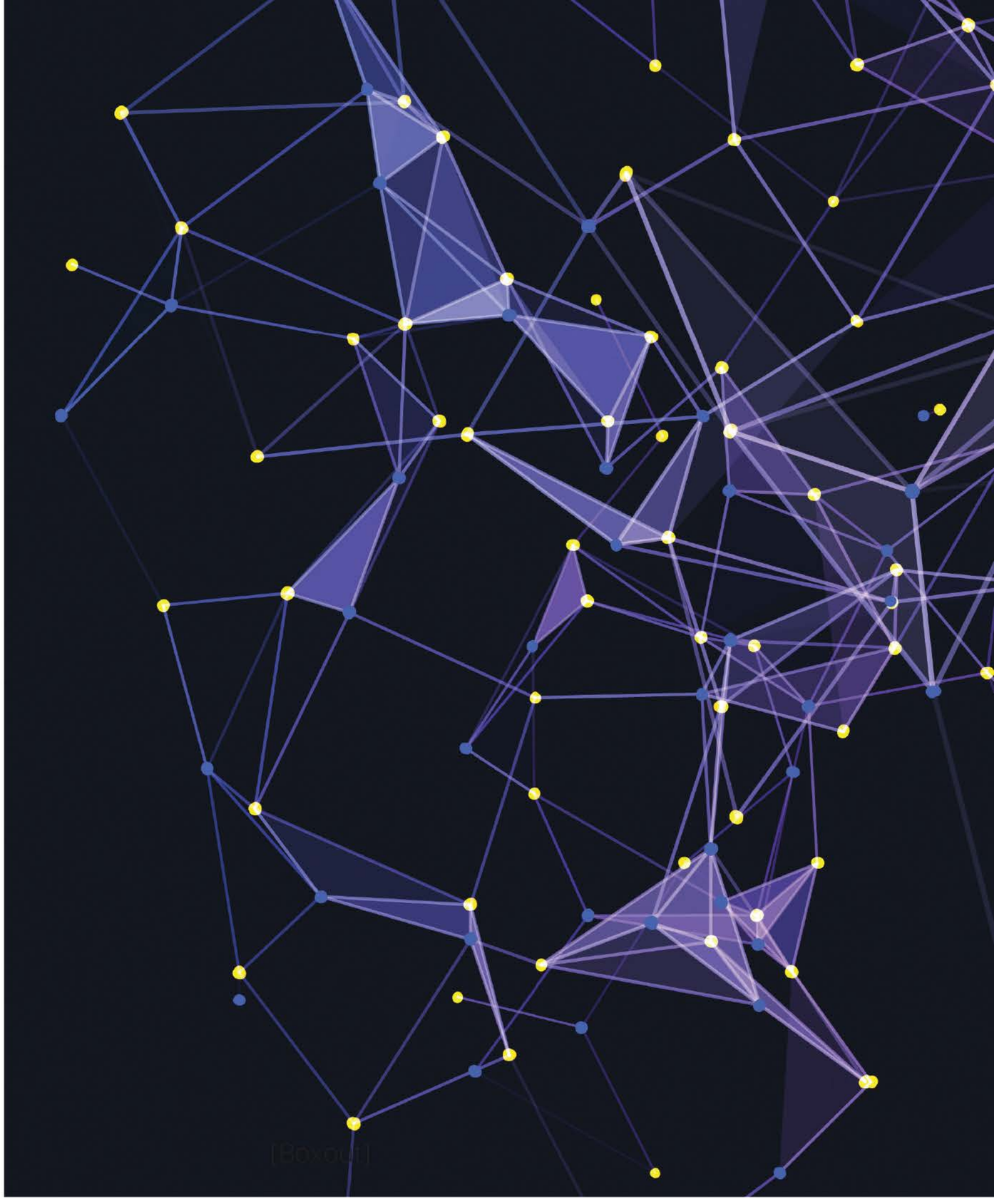
He views the challenge this poses for those working on connectors as exciting because "with technical architectural changes we are able to develop our in-house connectors faster. Along with the steady stream of connectors launched to market, we have also introduced Open Converter API. This will provide customers even greater flexibility, scale and control to post their custom datatypes directly to Global Relay for regulatory compliance".

Chind is similarly excited about the Global Relay Open Converter, which has a common interface to ingest both XML and API data flow. The new converter gets source data in various different formats and converts it to data for archive or to go back to the customer.

The logic built into the converter enables analytics features and the utilization of granular metadata; Global Relay is sharing its IP and features with its partners and customers so that their data is processed in the same compliant and rigorous way. This allows proprietary development teams to capture all their data for regulatory purposes. This means that files and data that were previously treated as one data point are now enriched with all the extra features that are available in the standard Global Relay archive.

It significantly widens the field beyond the established messaging and collaboration providers where there are already native connectors. This enables any application to take advantage of the data enrichment and archive features available for the larger data providers. This is the future for connectivity, where the APIs are designed to work for the underlying datatype.

One day all connectors will be built this way. ●



Six social media platforms have more than 1bn users each worldwide

Network evolution

The first social networking site was Six Degrees — it used the term to describe itself when it launched in 1997. But there wasn't a sufficient level of network connectedness to make it fly, and the platform was eventually sold off and subsumed into Youthstream Media Networks. Friendster went live in 2003 and was the first platform to engage at scale. But it couldn't satisfy demand and users began to migrate to MySpace, which also launched in 2003.

By 2006, MySpace was the most visited site in the world, and valued at $12bn. Two years later, Facebook took over as the number one social network. MySpace would eventually become a footnote in the history of social networking, alongside Orkut and Yahoo! 360°.

Social media platforms became tools you needed to use if you wanted to be part of the conversation. Everyone was more connected than ever before.

Kepios research estimates that if you factor in under 13-year-olds — who are restricted from registering to most social media platforms but who almost certainly still use them — then 78% of the total eligible global population regularly uses social media.

The regulatory STARS ALIGN

When it comes to operational resilience for outsourced services and critical third parties, there is a sense that global regulators are settling on a joined-up approach across all major territories

Words by
JENNIE CLARKE

Regulatory cohesion can be a thing of beauty. It doesn't happen often. Most of the time we are battling to put together pieces in a large and ever-evolving compliance puzzle. But every so often, global regulators appear to be on the same page.

When it comes to operational resilience, and especially as it relates to outsourced services and critical third parties, the regulatory stars are aligning.

Regulators from the EU, the UK, and the US are simultaneously working on new obligations and guidance that will set out expectations for firms looking to implement (or for those which have implemented) the services of third-party providers.

Regulatory standards for outsourcing are arguably long overdue. Over the past five years, outsourced services have become the norm for financial institutions. After all, no firm wants to build its own in-house technology only for it to become outdated by the time it is implemented? Of the many issues at hand regarding operational resilience and outsourcing, the consistent regulatory message appears to be one of accountability — namely that outsourcing a service does not mean the outsourcing of responsibility in the event of failure.

To quote SEC Chair Gary Gensler: "When an investment adviser outsources work to third parties, it may lower the adviser's costs, but it does not change an adviser's core obligations to its clients."

The issue here is that firms are gradually employing the services of more and more third parties. Those third parties also often use third parties to deliver their own services (fourth parties to the service recipient). Quickly, a web of third, fourth and even fifth parties is weaved, which can be catastrophic in the event of outages or disruption. Unless, that is, considerable due diligence is established at the outset. This is a risk to which regulators have slowly opened their eyes, with a raft of new and emerging regulation and some enforcement actions in certain cases.

A global pincer movement

The last year has seen a coordinated move for regulation and regulatory messaging around outsourced services, especially regarding operational resilience and due diligence. While regulators are not necessarily saying the same thing, they are focusing on the same areas, which is, at least, a start.

In the US, for example, the SEC has published proposed oversight requirements for investment advisers that outsource certain services. Under the proposed new requirements, which

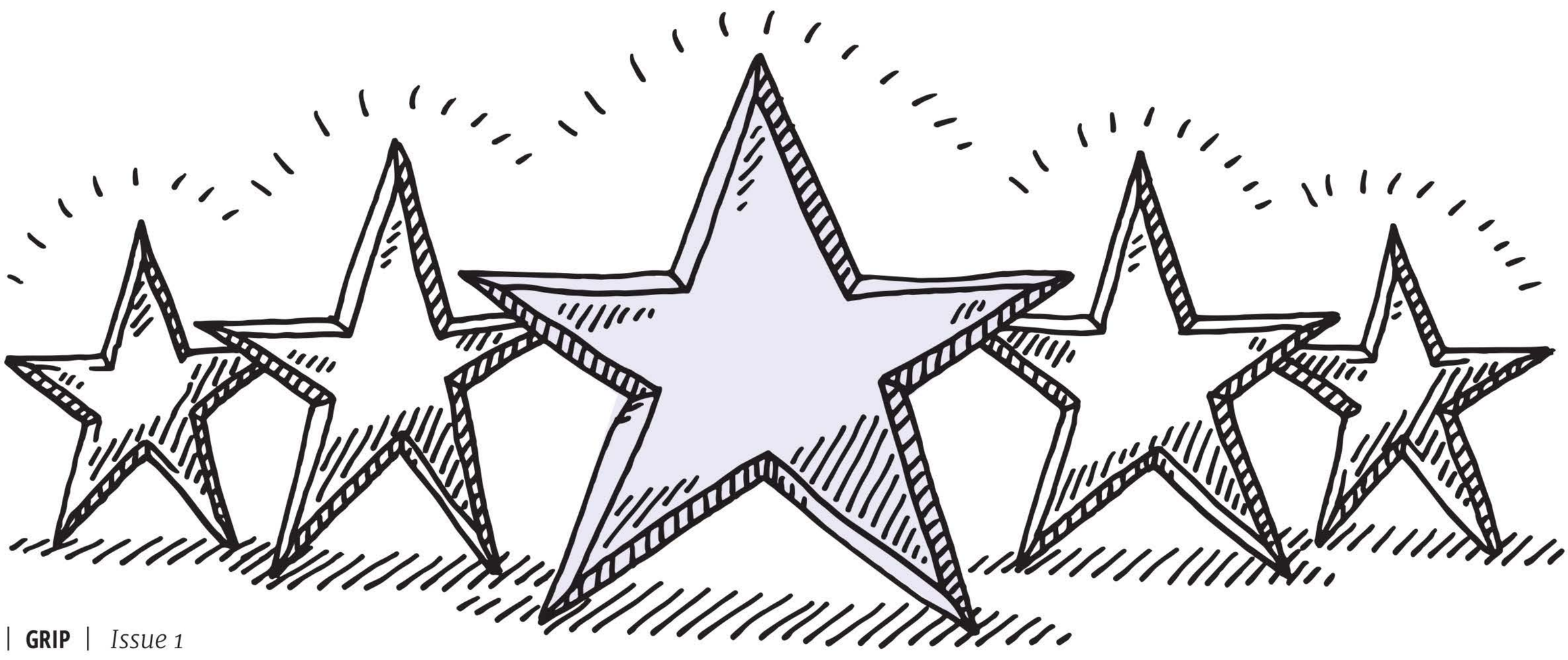


IMAGE: GETTY

are still under consideration, investment advisers would have to satisfy six new due diligence elements before outsourcing a service to a provider to perform certain advisory services or functions. These six new areas are:

- the nature and scope of services;
- potential risks, including their management and mitigation;
- the service provider's competence, capacity and resources;
- the service provider's subcontracting arrangements;
- coordination with the service provider for securities law compliance;
- orderly termination of the function by the service provider.

In the UK, on the understanding that financial institutions "increasingly rely upon third-party services to support their operations", we have seen regulators issue discussion paper DP3/22. Published in July 2022, it looks to establish a new framework for outsourced services that would:

- enable supervisory bodies to identify critical third parties;
- set minimum standards that these outsourced service providers should meet;
- create tools with which organizations can test the operational resilience of their outsourced vendors.

In the EU, many readers will be familiar with the Digital Operational Resilience Act (DORA), which is widely considered one of the most transformative pieces of legislation for operational resilience. Of the five key areas of focus for DORA, two concern outsourcing arrangements — namely the management of third-party risk and the arrangements surrounding information sharing.

Proof in the punitive action

Given the fast-growing tapestry of emerging regulation, it came as little surprise when in December 2022 the FCA and PRA issued £48.7m in fines to TSB Bank for historical operational resilience failures. Following acquisition in 2015, TSB embarked on a data migration mission on a mammoth scale. It had been planned for a number of years and in April 2018 the main migration event occurred. This faced technical errors, resulting in outages and leaving many customers and bank branches unable to access accounts and funds.

On investigation, the FCA and PRA found that TSB's data migration project failed for myriad reasons, most pertaining to ill-considered operational resilience:

- TSB prioritized meeting deadlines over adequate testing, meaning that some tests had been overlooked to meet certain timelines;
- TSB employed the services of a third-party vendor that had "no experience of managing service delivery from a large number of UK subcontractors" and failed to "explicitly address" the risks of using such a third party for a data migration of such proportions;
- TSB outsourced the project, which was "critical to the performance of TSB's regulated activities" but despite this, did not conduct a "formal, comprehensive due diligence exercise to understand [the third party's] capability to deliver";
- TSB failed to asses how the third party would deliver the migration project, therefore failed to understand that the third party was to use 85 third parties of its own (TSB's fourth parties) to carry out the migration;
- TSB failed to carry out business continuity planning for what would happen in the event the migration failed, meaning that business-as-usual was not restored until eight months after the outage event.

The case has piqued the interest of practitioners for a number of reasons, not least because UK regulators appear to have retroactively applied new operational resilience standards to the historical data migration project. At the time of the migration, many of the above operational resilience and due diligence expectations did not apply.

There is concern among some that this could set a precedent and prove challenging for many firms to meet. Not only must they adhere to stringent operational resilience standards for outsourcing moving forward, but must they also pore over historical projects to ensure compliance?

What does this mean for firms?

The future for operational resilience for outsourcing is clear, if not complex. Regulatory expectation and scrutiny will increase, firms will increasingly be expected to show significant and robust due diligence when outsourcing, and a third-party vendor must be prepared to provide significant information to prove its ability to deliver.

For now, firms should closely follow regulatory developments in anticipation of rigorous change. In the meantime, now is the time to take stock of existing and emerging third-party relationships.

Ask whether your third-party reliance can be consolidated. Look at processes and establish whether a single third party could do the job of many. If so, consolidate and reduce your net.

Can you show adequate due diligence? Do you know how your third parties are delivering your services? If you don't know, find out and plan business continuity to support this.

Have you tested for failure? What will happen if one of your third parties fails? As the TSB enforcement shows, regulators want to see testing prioritized.

Ultimately, operational resilience and outsourcing requires a fine balance. By all means outsource your services, but don't cast your net too wide. There remain many unanswered questions. For example, how far should you test a process and what happens if that process fails in testing?

The bad news is that future regulation will not make things easy at the outset. The good news is that things will be clearer as we move forward, and more firms may avoid outages and regulatory action further down the line. Prepare now, before you are in too deep. ●

> *"When an investment adviser outsources work to third parties, it may lower the adviser's costs, but it does not change the core obligations to its clients"*

BONFIRE *or* BLUFF?

Big Bang 2.0 and the Edinburgh Reforms

Will the UK government's Edinburgh Reforms deliver on the game-changing, Big Bang rhetoric or turn out to be more of a damp squib?

Words by
CARMEN CRACKNELL

IMAGE: GETTY

The second half of 2022 saw significant turbulence in British politics, with a government headed by Liz Truss lasting just 49 days. Following this, a spate of changes to City of London regulations — labelled the Edinburgh Reforms — was proposed in December.

Brexit breakaway

Billed 'Big Bang 2.0', in reference to the previous set of sweeping reforms and financial market deregulation of the original Big Bang in 1986, the latest spate is focused on Britain's post-Brexit future. Issues addressed include ring-fencing rules, ESG announcements, and Retained EU Law (REUL), all with the aim of taking advantage of "Brexit freedoms".

The UK government said this would include a commitment to make substantial legislative progress over the course of 2023 on repealing and replacing EU-era Solvency II, the rules governing insurers' balance sheets. This is expected to unlock over £100bn ($120bn) of private investment for productive assets such as UK infrastructure.

"The reforms are pragmatic in that they set out a flexible range of legal and regulatory mechanisms to transpose, amend or revoke REUL," says Martin Sandler, financial services regulatory partner at Eversheds Sutherland. "They prioritise the areas to be addressed into various tranches, and they set out a broad range of substantive areas of regulation to be improved and modernized in the process. A practical and flexible solution was required to deal with the large volume of REUL which was on-shored in raw, unadulterated form by the EU Withdrawal Act."

The Future Regulatory Framework (FRF) is another aspect of this, giving greater power to British regulatory authorities, namely the FCA and PRA. The media went as far as to dub Big Bang 2.0 a "regulatory bonfire". But opinions in the financial services sector are that reforms will not be as far-reaching as the government says.

"I'm sceptical that any of this will make a change for the vast majority of UK financial services firms, because so many of our rules are baked into everyday conduct of business activity conducted by firms," says Tim Dolan, Shareholder

I'm sceptical this will make a change for most firms, because many rules are baked into everyday conduct"

and Partner at Greenberg Traurig, in an interview with *GRIP* (full interview, page 20). "To remove some of them now would actually create more administrative hassle for very little benefit. What I think will happen is that there will be changes around the regulatory capital regime for insurers and other very large institutions, but not for the vast majority of firms."

One of the government's main stated aims is to boost growth in British industries, including digital technology, life sciences, green industries and advanced manufacturing. "If anyone is thinking of starting or investing in an innovation or technology-centred business, I want them to do it in the UK," the Chancellor Jeremy Hunt said in January. "I want the world's tech entrepreneurs, life science innovators and clean energy companies to come to the UK because it offers the best possible place to make their vision happen."

Whether these reforms will facilitate this remains to be seen. "We have an overworked regulator with some firms being authorized to do things that don't require authorization," says Dolan. Despite this, he says FCA has developed ESG labelling that is "more pragmatic" than EU-developed categories.

One aspect of the proposed reforms was the change to ring-fencing regulations, a piece of legislation that came into force in 2019 that requires the largest UK banks to separate core retail banking services from their investment and international banking activities.

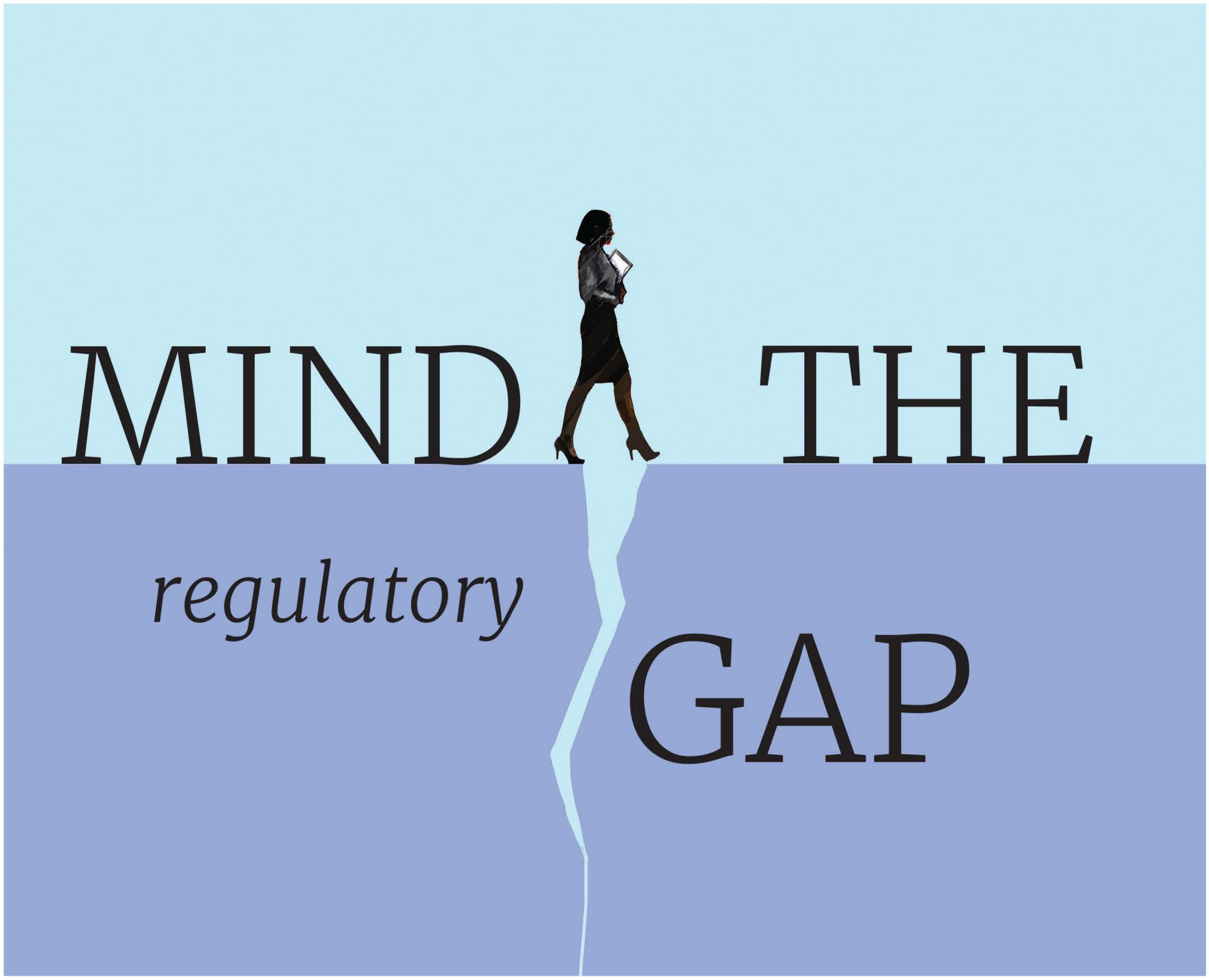
"In terms of ring-fencing, there may be savings or gains for very large institutions around capital. It's very sensible. But it won't move the dial for the vast majority of authorized firms," Dolan adds.

The Edinburgh Reforms are due to come into force in mid-2024. ●

What's in Edinburgh?

The Edinburgh Reforms package is an exhaustive, and potentially exhausting, range of measures covering various aspects of the financial services regulatory landscape. Taken together they would represent the Big Bang 2.0 that has been promised. So what are the most striking, and potentially most important, aspects of the reforms?

1. **Reforming the ring-fencing regime for banks.** A major step, that would mean savings for some larger institutions, but not that significant for most authorized firms.
2. **Issuing new remit letters for the PRA and FCA** with clear, targeted recommendations on growth and international competitiveness. This could be significant, but will also be difficult to enforce.
3. **Commencing a review** into reforming the Senior Managers and Certification Regime in Q1 2023.
4. **Committing to having a regime** for a UK consolidated tape in place by 2024.
5. **Repealing the Packaged Retail and Insurance-based Investment Products** (PRIIPs) Regulation, and consulting on a new direction for retail disclosure. There is demand for this.
6. **Publishing the plan for repealing and reforming EU law using powers** within the Financial Services and Markets Bill, building a smarter regulatory framework for the UK. It isn't immediately clear how this will be done, or why this is included.
7. **Launching a Call for Evidence on reforming the Short-Selling Regulation.** Again there is little detail on the intention here.
8. **Consulting on removing burdensome customer information requirements** set out in the Payment Accounts Regulations 2015. This is welcome, although it may tip the balance too far the other way.
9. **Establishing an Accelerated Settlement Taskforce.** This matters but there is no detail or timetable.
10. **Increasing the pace of consolidation in defined contribution pension schemes.** This is important but there is no indication of how it will be done.
11. **Improving the tax rules for Real Estate Investment Trusts from April 2023.** There is no indication of how this will be done.
12. **Becoming a world leader in sustainable finance.** The government is ensuring the financial system plays its role in the delivery of the UK's Net Zero target and wants the UK to be the best place in the world for responsible and sustainable investment. It will publish an updated Green Finance Strategy in early 2023 and consult in Q1 2023 on bringing ESG ratings providers into the regulatory perimeter.
13. **A sector at the forefront of technology and innovation.** The government is ensuring that the regulatory framework supports innovation and leadership in emerging areas of finance, facilitating the adoption of cutting-edge technologies. This includes, among other ideas, consulting on a UK retail central bank digital currency alongside the Bank of England.
14. **Delivering for consumers and businesses.** The government is continuing to work with the regulators and industry to ensure the sector is delivering for people and businesses across the UK. As part of this it is consulting on Consumer Credit Act reform and laying regulations in early 2023 to remove well-designed performance fees from the pensions regulatory charge cap.



We spoke to financial regulation lawyer **Tim Dolan** about the Big Bang 2.0, ESG, crypto, and the regulatory challenges that lie ahead in different jurisdictions

Words: **CARMEN CRACKNELL**

G In terms of Big Bang 2.0 and Brexit freedoms, what key pieces of financial regulation are coming for the UK?

I'm skeptical that any of this will mean much of a change for most UK financial services firms, because so many of our rules are baked into everyday conduct and business activity of firms. To remove some of them now would create more administrative hassle for very little benefit. What I think will happen is that there will be changes around regulatory capital regime for insurers and other very large institutions, but not for most firms.

While there could be some efficiencies gained and maybe some changes around the freeing up of capital markets in the UK, for a typical FCA-authorized firm I suspect there will be very little benefit whatsoever.

It is worth remembering that a lot of the European infrastructure we are still dealing with has its genesis ultimately in the UK and the UK regulatory body.

G Is there a gap between aspirations and the practical implementation of regulation?

There is a huge gap between what we need to be regulating and what we are regulating. In my view, we are almost completely dependent on a framework that was created in the mid-1980s, following the Big Bang, which has since had layers added to it.

But in that time there has not been a fundamental discussion about what we regulate, why we regulate financial institutions, what we are seeking to achieve from that regulation, what we need to regulate, how many people we need, and the cost of that regulation.

We haven't had that discussion ever about what it is we are regulating and why. Therefore, we work with a rulebook and set of legislation designed to capture activity before the electronic age, which when you think about it is extraordinary.

A lot of the language we use in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 is connected to the concept of people having physical rather than electronic contact with each other, be that with a product provider, manufacturer or customer. That is the bit that's sorely missing with regulation and where the gap lies.

G Do you envisage an attempt to update the framework in the near future?

Not with the latest version of this government. There might have been earlier this year, but now I get the sense that probably not. You almost get the sense the government might be nervous tinkering with things they feel they don't need to tinker with.

But it needs to happen at some stage because we have an overworked regulator with some firms being authorized to do things that don't require authorization, while at the same time we have this constant clash between what it is we are trying to achieve from regulation. Is it about protecting consumers or an efficient market? Is it financial stability and confidence or is it something else? Often you have the regulator trying to be all things to all people — and it can't do that because it doesn't have the resources.

"There is a huge gap between what we need to be regulating and what we are regulating"

G What about ESG?

The European Sustainable Finance Disclosure Regulation (SFDR), has been in place for more than a year now, but a fundamental problem has developed. It was supposed to be about improving transparency around what investment products are doing and what they are investing in; the idea in Europe was that if a product promoted ESG criteria or was fixed to a benchmark, then it would be in one of two different categories.

The issue is that SFDR has become a labelling regime — something it wasn't designed to be. Investors, consumers and product manufacturers are all questioning whether a product falls within Article 8 (which captures products that promote ESG concepts) or Article 9 (which captures products that are actively pursuing ESG and have agreed to be fixed to a specific benchmark by which they will be held accountable) or possibly an Article 6 product, which is not pursuing ESG at all.

It sounds well and good, but the framework itself is not designed for that sort of labelling.

G Is there a difference in ESG labelling between Europe and the UK?

The disclosures that are required just don't work properly for a labelling machine. By contrast, we have the FCA consultation paper that came out recently, in which there are labels the FCA has developed that are more pragmatic.

They talk about more sustainable-focused products aiming to invest in assets that can be reasonably regarded as being ESG-sustainable, or sustainable improvers that are aiming to invest in assets with the potential to deliver improvements in ESG criteria, or sustainable impact, which are products that are going to achieve a measurable ESG outcome themselves.

That to me seems more workable, more focused on the underlying investor or consumer and what they want to try to understand.

The UK regime won't come into force until mid-2024, but in the future you will have products that are potentially offered in Europe and the UK making quite different disclosures, which doesn't help anybody. The challenge, though, is that we now have this gulf between the European and UK regime.

To state the obvious — understanding and pursuing ESG at the highest level must be a good thing and having structures in place to avoid or ensure companies do not greenwash is a good thing. So I guess it follows that at the highest level that helps make companies more resilient.

G Moving on to crypto, how will regulation evolve in that sector in different jurisdictions and does there need to be cohesion?

My fear is that we will continue to have a disjointed response to crypto. My hope would be that we have one consistent way of understanding and regulating crypto around the world, but I suspect I'm being too naïve in that regard. It's impossible to predict. What we do know is that most standard regulation around the world has been created following a crisis or a problem, and with the relatively recent developments overseas, that may lead to the conclusion that global regulators need to do more than they're doing and lead to something happening.

I hope something does happen, as for the moment we're in a no man's land, which isn't helpful for anybody. If there was more regulation of crypto that would help the crypto sector itself with regards to consumer confidence. I'm in the camp that thinks it must be regulated and that not all crypto is a scam. It is clear to me that crypto can be used quite legitimately for legitimate purposes. ●

At the time of interview, Tim Dolan was a Partner in the financial services regulatory lawyers team at Reed Smith. He has since has moved on to become a Shareholder at Greenberg Traurig.

ONE RULE

that's finally ringing the changes

The SEC has made amendments to recordkeeping Rule 17a-4 for the first time in 25 years. What do the changes mean, and how can firms prepare?

Words by
JENNIE CLARKE

Think back to 1997… You probably didn't have a mobile phone. The computer you used would look ridiculously large in today 's office, but had less computing power than your current TV remote control. And who could ever forget the high-pitched internet connecting dial-up tone?

We may not like to admit it, but 1997 was a long time ago. So it is surprising that one of the US Securities and Exchange Commission's (SEC) primary recordkeeping rules — Rule 17a-4 — has not been updated since then. That is, until now. Rule 17a-4 outlines the requirements for data retention, indexing, and accessibility for regulated entities that deal in the trade or brokering of financial securities. It obliges firms to ensure the retention and preservation of all transactions and official business records, including all communications.

Despite being the governing force behind record retention, the rule is facing its first revision since it was amended in 1997 — when faxing was the most common form of business communication — to allow for electronically stored records. Fast forward a quarter of a decade and we have witnessed revolutionary technological change worldwide, from the roll out of wifi to data storage in the cloud.

What is changing?

On October 12, 2022, SEC chair Gary Gensler issued a Statement on Final Rule Amendments to Electronic Recordkeeping Requirements. Within that statement, he confirmed the final changes that are designed to "modernize" the electronic recordkeeping requirements. He noted that the new Final Rule, if adopted, "would bring the Commission's electronic recordkeeping requirements in line with technological innovation".

Alongside the 146-page Final Rule, the SEC has published a fact sheet that clearly delineates the rules affected by the amendments:

- rules 17a-4(f) and (j) under the Securities Exchange Act of 1934 which govern the electronic recordkeeping and prompt production of records requirements for broker-dealers;
- rules 18a(6) and (g) that set out the electronic recordkeeping and prompt production of records requirements for security-based swap dealers (SBSDs) and major security-based swap participants (MSBSPs);
- rules 17a-4(i) and 18a-6(f) concerning the provision of records to the SEC by a firm or third party.

The amendments mean myriad changes for the way firms manage data. In particular, there are three major updates; removing the WORM requirement, allowing for in-house recordkeeping to be handled by an elected in-house designated executive officer (DEO), and new obligations for SBSDs and MSBSPs.

Removing the WORM

Under the previous iteration of Rule 17a-4, firms had to ensure that their data was exclusively preserved in a non-rewritable and non-erasable format — known as 'Write Once, Read Many' or 'WORM' format. This generally meant that recordkeeping should take place through the medium of then-pioneering technologies, such as CD-ROM.

But data storage and recordkeeping technology has evolved in lots of ways since, and under the amendments, the WORM format will no longer be required. Instead, brokers are given alternative methods of data storage, including storing it on their own servers or those of third parties. The critical points are that:

- the preservation of records must have an audit trail;
- the SEC will need to be able to access the firm's data;
- any new system must ensure all business records (including communications data) is preserved in an electronic manner that allows for the recreation of the original, even if that original has been modified or erased.

IMAGE: GETTY

Offering an in-house alternative

Under the existing rules, broker-dealers are asked to hire a designated third party (D3P) that has access to the firm's data. However, the amended Rule 17a-4 provides an alternative so that, instead of electing a D3P, firms can elect an internal DEO and bring the obligation in-house.

This adds greater flexibility to brokers when considering their recordkeeping requirements. Whether firms have elected a DEO or a D3P, they will be required to have access to the firm's electronic records and to provide those records to the regulator where the firm fails to or is unable to do so.

Obligations for swaps

The amendments to Rule 17a-4 also mean that, for the first time ever, SBSDs and MSBSPs will be subject to the SEC's requirements.

> *"The modernization adds flexibility to address new technologies, such as the cloud, that firms use to store records"*

This update is long overdue and will benefit lots of different firms, by offering flexibility and innovation in the way they retain, index, and access electronic communication data.

For a long time, firms have struggled to understand and to comply with the SEC's recordkeeping rules, given that tech solutions have developed way beyond the scope of Rule 17a-4.

The changes will likely offer much needed clarity, as well as what Gensler highlighted as the "flexibility to address new technologies, such as the cloud, that firms use to store records".

He also noted that the amendments could have cost advantages, too.

For example, firms that already use audit-trail technology for their day-to-day records may now use the same solution to comply with this rule, rather than feel on the 'hook' to keep separate, WORM-compliant records.

A time for action

The final amendments to Rule 17a-4 come into effect 60 days after publication in the Federal Register.

The compliance date, however, differs for broker-dealers, MSBSPs and SBSDs, presumably to give those less prepared more time to comply. Broker-dealers will have six months to comply from the date the amendments are published in the Federal Register, while MSBSPs and SBSDs will have a total of 12 months.

During this transitional period, firms should consider how best they want to utilize third parties to meet recordkeeping requirement obligations and whether they wish to elect a DEO as an alternative.

It is likely that the new role of a DEO will be onerous, given that they will be expected to maintain the same unwavering standards as a highly trained, experienced D3P firm.

Firms should also take stock of the technology they are currently using to maintain recordkeeping requirements and explore its suitability to keep up with the amended rules.

For example, does your recordkeeping archive allow for functional searchability and eDiscovery? And do you have the tools you need to meet regulatory disclosure and audit trail requirements when requested? ●

MARKET ABUSE

coverage in the spotlight

Alex Viall discusses significant market abuse enforcement actions from the UK's Financial Conduct Authority last year and the impact they are having on regulated firms, with **Aaron Stowell**, Partner of Forensic Technology and Surveillance, KPMG

Words: **ALEX VIALL**

AV: Give us an overview of regulatory tolerance and process, after a flurry of market abuse enforcement in 2022? Has regulatory expectation shifted and are we entering a new phase for enforcement?

AS: Banks are just being fined now for things that happened so long ago historically. These are lapses that happened in 2018 and before in some cases. Several organizations are still dealing with, or feeling the impact of, Fed orders. Regulators are taking less of a positive view on organizations presenting what they are aiming to do.

Regulators want to see a clear action plan to close gaps, they don't want to hear 'we'll improve our overall recording, voice capture and detection program'. I am sure regulators would argue there are vendors offering proven solutions, so why are you not doing it? They are aware of peer benchmarks, see people conquering voice to text, even video capture and detection. Regulators can point to others in the market who are doing this now, at scale, many for several years.

AV: Is this change in regulatory supervision attitude universal among regulators?

AS: That's difficult to analyse. Looking just at the FCA, it has issued larger collective fines in previous years (2019 and 2021) than last year. It also had quite a focus on financial crime last year, so I wouldn't say the FCA was necessarily being more aggressive or focused on any specific areas. Some of these failures related to basic things, and I don't think it is unreasonable to assume that internally some of these cases have been pending for so long that the underlying issues should have been resolved. Five years is long enough.

None of the market abuse fines from last year seemed disproportionate. I was surprised by the size of the Sigma fine, £530,000, which was at the low end of the scale — it was reported as a number of potentially suspicious transactions and orders that went unreported. The £5m (BGC) and other fines were indicated to have been influenced by repeated failures.

Despite remediation, elements of the core problem and design failures seem to have remained after that period of remediation. What options does a regulator have in those circumstances? The fines did not seem out of proportion, especially when compared with the new benchmark from the SEC and CFTC under recordkeeping enforcement. I don't currently see a change in attitude demonstrated by all regulators.

There is a sense that the volume of regulatory change, along with newer challenges such as crypto regulation, are substantial. But in many cases the required regulation has been in place for an extended period. These fines seem to

be intended to inform the market that these things are achievable, and with relative ease. Excuses don't land well any more, if they ever did.

AV: What are clients asking for as this all washes through the market? Is there a commonality in demand and approach or is it varied and unstructured?

AS: A real variety, and it depends on the strategy of a particular company and where they feel they are strong or weak currently, what they have in place from a technology point of view, and if they are under any type of order with existing areas that have been identified as 'in need of improvement'.

The scope ranges from policy and procedures to how organizations are capturing, recording, and validating data from the surveillance first line, moving into supervision. There is introspection – 'are we confident that this approach is actually meeting requirements?'

For some it is just a technology play where the main focus is on actual capture, and we may help assess vendors or enhance existing audio processes.

I see different aspects from last year's fines, some brokers might be scrambling to adapt to new expectations, but I have not yet seen the same with asset managers, which is a surprise. Many brokers handle an extensive area of business via the phone and quality of capture and more importantly monitoring is easy to get wrong. There is a lot we can do to help get that up to the levels of the best peer performance. I don't think asset managers are immune in this area, with extensive call use and being open to the same weakness in systems and controls. I expect to hear more in this area, after the Amundi fine.

AV: Are you finding this is across tiers or types of firm, whether defined by size or sector, in terms of needs and movement and, to some extent, paranoia?

AS: Everyone is picking up on this. It depends on where the organization is right now. I have seen some tier twos in a better place than some tier ones owing to previous investigations and remediation obligations. Everyone on the sell side is taking it seriously and looking to do something with quite aggressive time frames where they still have gaps. I think we might see a lot of change in the communications monitoring industry in the short term, as we have seen the loss of the Relativity Trace application, and I feel there may be pressure on other private equity-funded players — so there might be some more departures or consolidation.

The standout businesses have a very clear view of what they want to achieve, how to move this space forward, bring improved results and increased value, and what they can offer to their clients. Banks are now looking for so much more from vendors beyond pure monitoring — they want real value and insight for all of that spend. They need to do more with all of their information.

AV: Are people just throwing money at the problem in terms of tech and new personnel and consulting assistance, or is it not at that stage yet?

AS: It depends and is related to confidence in existing teams and their ability to do this internally up to a point. But it is a very cost-conscious market right now. If there is not an obvious answer and a firm feels it's behind its peers, that is not a comfortable place to be. Regulators are messaging that this is not that complex — anyone suggesting a timeline of 18 months-plus to remediate, that won't wash. They need to engage, whether that is internal teams, consultants or vendors.

> *"The standout businesses have a very clear idea of what they want to achieve ...and what they offer clients"*

AV: Have you detected regulators requiring more evidence of market abuse monitoring compliance and a semi-informal reporting requirement that feels like a new informal obligation?

AS: I am not close to this area of the market, so it is hard to say. But this would be a natural development. If you are focused on getting value for money and protecting your firm, you start to remediate what you are monitoring and collecting and what your process is.

Then supervision is the next focus as that is when you can correct based on all the information you have gathered. People can end up wasting time analyzing reports that bring no value.

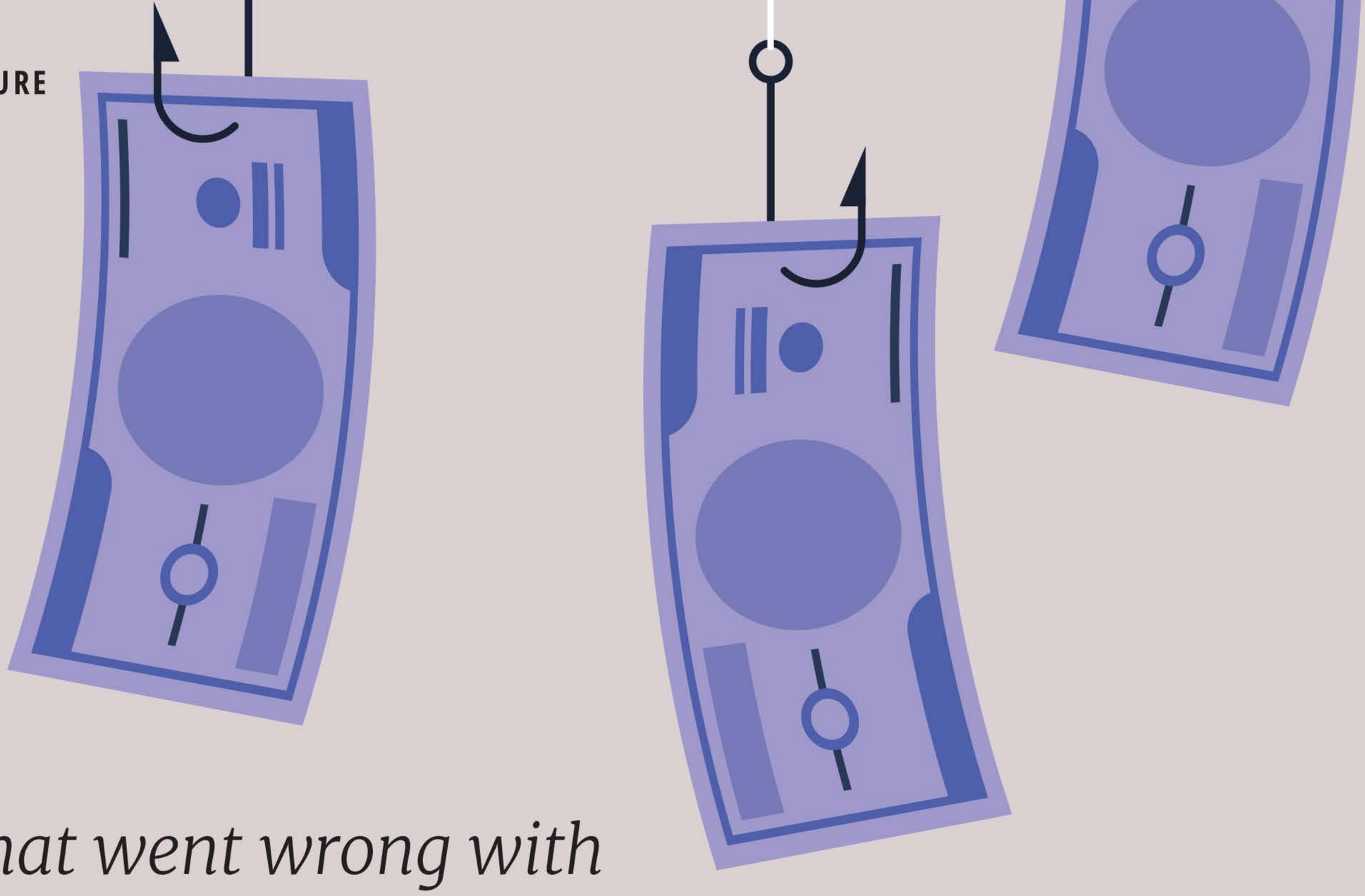
Certain banks I know are very focused on this as it fits their strategy. Others might be further behind but will get there as this is how you get to really change things positively.

AV: What advice can you give right now to ensure risk mitigation, adapting to this new environment?

AS: It starts by asking yourself whether you are really confident in your existing process. Is it doing what it is trying to achieve and how successful is it? Organizations have all of these stages and the steps that they have to go through, but the actual aim and clarity needed for each step and the overall outcome is often absent.

Behavioral analytics in supervision is an often-discussed topic, but there are so many challenges — such as the ethics of this approach, the quality of that data, the siloed information — that it feels like a veil. The key is what you need to monitor and supervize and what will make the process better and why, stripping away these other layers. You need a strategy to be able to present to a regulator on why you are confident that your approach provides the protection you are seeking.

I am not convinced everyone has that in their program. It is a simple process to continue to build on what has gone before. Some firms are still relying on what was put in place before 2015. But is that still relevant? Things change and it is key for everyone to reassess regularly. ●



What went wrong with WIRECARD?

The implications of Germany's biggest post-war financial fraud

Words by
BEN EDWARDS

At its peak, German payments company Wirecard was worth €24bn ($25.4), more than Deutsche Bank. It was the darling of the German fintech industry — proof that German fintech startups could compete with the world's biggest tech companies.

And then it all unraveled. In June 2020, the company was forced to admit that half of its revenues and almost €2bn ($2.1) of cash it previously claimed was sitting in bank accounts in Asia did not actually exist. Wirecard immediately collapsed into insolvency, causing billions of euros in losses. CEO Markus Braun was subsequently charged with fraud, while chief operating officer Jan Marsalek is still a fugitive on Europe's most wanted list.

The fraud lays bare a litany of systemic failures across multiple institutions, from a lack of internal accountability and external and internal auditors who were caught napping, to regulators who were too eager to believe and investors who were blindly following the herd.

As the court case plays out in Germany and the finger pointing about who is to blame continues, the autopsy on what went wrong and why is starting to shed some light on events.

The first line of defense that failed was Wirecard's own internal controls. While it can be challenging for lower-level risk managers to police the c-suite if they are conspiring to hide a fraud, the management board should have sufficient independence to provide proper oversight and question if something seems off.

"It is the duty of the board to establish a compliance system and make sure it works," says Gunther Friedl, a professor of management accounting at the Technical University of Munich. "One of the problems was that the internal controls did not develop at the same speed as the growth of the company."

Internal controls are also likely to fail if the person at the helm of a company has an overbearing character who makes it difficult for others to push back against.

"Germany is now finding exactly what the UK found during the financial crisis of 2008, which was if you have a dominant personality on a board, then effectively the entire structure breaks down," says Sara George, head of white collar crime and partner at Sidley Austin.

"If you have dominant personalities who dictate everything and there is nobody around them who's willing to go and challenge or kick the tires, then this is what can happen."

IMAGE: GETTY

Regulatory failure

External auditors also failed to uncover what was going on, missing at least one opportunity to catch the fraud by not checking balances in those bank accounts in Asia.

"Essentially, [auditors] EY used the information provided by Wirecard to contact bank personnel and verify the billions of dollars in cash that was supposedly in these accounts rather than independently confirming it," says Mason Wilder, a research manager at the Association of Certified Fraud Examiners. "The analogy I like to use is that EY fell for the time-honored ruse of giving your roommate's number as a job reference and saying this was my boss at my last job and he'll tell you all about how great I am."

The German banking regulator BaFin also failed to identify the fraud. Indeed, when the scandal was first reported in the *Financial Times* newspaper, instead of investigating Wirecard, the regulator filed a criminal complaint against Dan McCrum, the journalist who broke the story following a tip-off from whistleblower Pav Gill, a former in-house lawyer at Wirecard. Incredulous that the country's global fintech star was a fraud, BaFin claimed Wirecard was the victim of a scheme hatched by short-sellers. That reaction mirrored a broader blind spot in Germany — everybody wanted to believe that Wirecard was the country's answer to the tech successes that were coming out of the US and China.

"The whole of BaFin and everyone around Wirecard, including [the then Chancellor] Angela Merkel, were being told the emperor was fully clothed," says Jane Jee, who leads the financial crime project at The Payments Association. "I'm sure some of them had doubts, but they didn't want to be the one that said he hadn't got any clothes."

Save for some determined short-sellers who were unconvinced about Wirecard's purported numbers, many investors were also eager to buy into the company's story without asking too many difficult questions.

"There was a lot of fear of missing out and some of those pitches sounded pretty good, which the average investor might not have the technical expertise to dissect," says Wilder. "If you combine that with the willingness of leadership to conduct financial statement fraud to make those numbers look even better, it's easy for investors to get taken advantage of — especially when you've got one of the biggest accounting and consulting firms in the world signing off on things."

> *"The whole of BaFin and everyone around Wirecard were being told the emperor was fully clothed. They didn't want to be the one that said he hadn't got any clothes"*

One lesson from the Wirecard case and other frauds involving supposedly innovative companies is that in their high-tech complexity, regulators, auditors and investors sometimes focus on the wrong things and fail to ask simple questions.

"There is no such thing as a question that is too basic," says Jee. "You must ask them how they make money. Asking what their business model is doesn't necessarily involve telling you how they make money."

Another sign something could be awry is if a company seems to be performing unfathomably better than its peers.

"Wirecard was doing too well," says Jee. "I've worked at WorldPay and I've worked at Trust Payments, and I understand payment processing and the money that comes in from it. So you have to ask, what was Wirecard doing that was so different from its competitors and why was it making so much more money?"

Spotting future fraud

Researchers at Friedl's university are currently developing technology that could identify potential future frauds by searching for hidden fingerprints in a company's accounts that may signal something is suspicious and should be investigated further.

"This algorithm would have been able to detect the Wirecard case with an 80% probability," says Friedl. "It's looking at the balance sheet data, profit and loss data and cash flow data and then comparing it to other fraud cases. It couldn't be identified by simply looking at the individual balance sheet but it can be identified by looking for patterns that are similar to previous fraud cases."

While the full implications of the Wirecard fraud are still playing out in the courtroom, George believes there should be an investigation in Germany into the regulatory response.

"BaFin really has to show some willingness to examine and be self-critical about how this was able to happen and why the fraud wasn't identified," she says.

The case is also likely to have far-reaching implications for EY and the other big accountancy firms, which were already under scrutiny for the lack of separation between their audit and consulting arms.

"Conflicts of interest were endemic in the accountancy industry, where audit work was seen as a way of introducing other services. The consequences of that are now being realized," says George. "Most audit failures are very simplistic. Often the relationship is a little too cozy and they don't independently verify information. There has been a real recognition that what people think an auditor is doing and what auditors actually are doing are quite different when it comes to fraud."

While Wirecard might leave a lasting legacy on the regulatory and audit front, the recent collapse of crypto exchange FTX underscores the ease at which high-flying tech startups promising to revolutionize their respective markets continue to dupe a broad range of stakeholders.

"Wirecard was really on the front-end of this series of fintech issues and scandals that we have seen with some of these crypto companies and decentralized finance platforms that have since gone under," says Wilder. "Regardless of what else happens now with Wirecard, it's always going to be a big cautionary tale. If something sounds too good to be true, it generally is." ●

Get the motor RUNNING

Motor insurance has been at the sharp end of a lot of regulatory scrutiny. Despite this pressure to behave responsibly, it's still not clear if UK drivers are getting the best deal

Words by **MARTIN CLOAKE**

It is not surprising that car insurance has been prominently in the sights of UK regulators. The UK market is the third largest in Europe — behind France and Germany — with €20bn ($21.4bn) of the €100bn ($107bn) gross written on premiums in Europe in 2021. Perhaps more importantly, it's a compulsory purchase if you drive a car. And at the last count there were some 31 million registered drivers in the UK.

Taking the slow road

Regulators have for some time been taking action to ensure consumers get a good deal. Way back in 2014, the Competition and Markets Authority (CMA) published a series of measures it said would "increase competition in the car insurance market and reduce the cost of premiums for drivers".

These included a ban on agreements between price comparison sites and insurers that stopped insurance firms making policies available more cheaply on other websites, and recommending the Financial Conduct Authority (FCA) looked at the quality of information about products sold as add-ons.

Seven years later, in 2021, the FCA introduced measures to prevent price walking — the name given to the process by which insurance companies increase the price of car and home insurance premiums for existing customer, allowing them to offer cheaper deals to entice new customers, essentially a tax on loyalty. The FCA estimated these measures would save £4.2bn ($5bn) over 10 years and make the market work better.

But only last year, the FCA felt the need to warn car insurers not to offer prices under fair market value when settling claims. It wrote to companies telling them to handle claims promptly and fairly, and to consider the cost of inflation when settling. This ties in with the work the regulator is doing to enforce the new Consumer Duty, which requires firms to deliver "good outcomes" for customers.

Driving up prices

But despite the regulator's efforts, nine years on from the CMA investigation and after multiple interventions, research by price comparison outfit Confused.com reveals that car insurance premiums have

risen 19% — the biggest annual rise in six years. UK motorists now pay an average £629 ($754) a year to insure their cars.

The road less traveled

So, how effective have the efforts of regulators been at delivering a better deal? The FCA issued a statement at the end of last year headlined "New year delivers fairer home and motor insurance renewals", with Sheldon Mills, the regulator's executive director, consumers and competition, saying: "Our interventions will make the insurance market fairer and make it work better. Insurers can no longer penalize consumers who stay with them. You can still shop around and negotiate a better deal, but you won't have to switch just to avoid being charged a loyalty premium."

The regulator also says it has secured redress for consumers in a small number of cases where companies had accidentally price discriminated against loyal customers, and has published research showing not only that long-standing customers were still being discriminated against, but that poor recordkeeping meant many insurance companies could not prove they were not price discriminating between new and existing customers.

Smaller firms, in particular, "had few or no records to show how they had complied with our pricing rules" and "in most cases no evidence or records were provided to substantiate how these firms had satisfied themselves that they were and are complying with our pricing rules". Larger firms "were generally able to show that they had taken appropriate actions to comply" but "not all the information that was reported to the person responsible for the attestation was made available to us". The research also highlighted the fact that many firms had not appointed enough staff at a senior enough level to judge properly whether the business was complying with requirements.

> *Our interventions make the market fairer. Insurers can no longer penalize consumers who stay with them"*

Keep your eyes on the road

All of this could be put down to teething troubles for a new regime. But seasoned observers question whether the focus is right. "Insurers should be looking more at controlling claims costs and ensuring people don't get away with it," says Branko Bjelobaba, a general insurance specialist and former vice-president of the Chartered Insurance Institute. "What insurers spend on claims we, the insurance buying public, have to pay for in our premiums."

In 2020, the last year for which complete records are available, motor insurance companies paid out a total of £13.5bn ($16bn) in claims. And you don't have to go far to find evidence of repair shops quoting for parts replacements when a repair would be cheaper.

Costs for insurers are rising and the difficulties companies face were underlined when Direct Line, the second biggest player in the UK market behind Admiral Group, announced it was scrapping its dividend payment because of the rising cost of claims. Margins are thin to non-existent, with S&P Global quoting sources who expected the industry combined ratio to be "significantly above 100% for 2022 and 2023". That means insurers paying more in claims than they receive in premiums.

Car insurers, in particular, face unlimited risks, as Chris Wheal, former editor of *Insurance Times,* explains. "If a driver falls asleep at the wheel, leaves the road and ends up on a train track, causing a train crash, the costs will run into billions. That all comes on a £450 ($539) insurance policy," he says. The combination of huge risk, claim inflation and a decreasing ability to use price increases as a defense means that insurers are deciding "it's not worth it".

Encouraging consumers to shop around is only effective if there are alternatives to shop around for. But current market conditions mean choice is, if anything, being reduced.

> *The regulator's focus is to make it cheaper, but they should focus on making it simpler"*

In Wheal's view, "the regulator's focus is to make insurance cheaper, but it might be better if they made it simpler". It's very hard, he says, for the average person to know if they are properly insured. He gives an example of a physiotherapist who also provides training. If they have an accident on the way to provide training rather than physiotherapy, they are not covered unless they have specified 'trainer' as a second occupation on their policy.

A broken market

Wheal is pessimistic about the market, saying: "Insurance is a broken model. Demutualization has done a lot of damage. And regulation doesn't allow for the law of adverse consequences."

To illustrate the point he says: "The FCA brought in the Insurance Conduct of Business Source Book requiring tough standards on those who recommend financial products and lower, more relaxed rules for those not giving advice. Now most firms that call themselves 'brokers' have withdrawn from giving advice at all, to make complying with regulation much cheaper. They sell unadvised. It is entirely down to the buyer to decide if the cover is appropriate and the price fair.

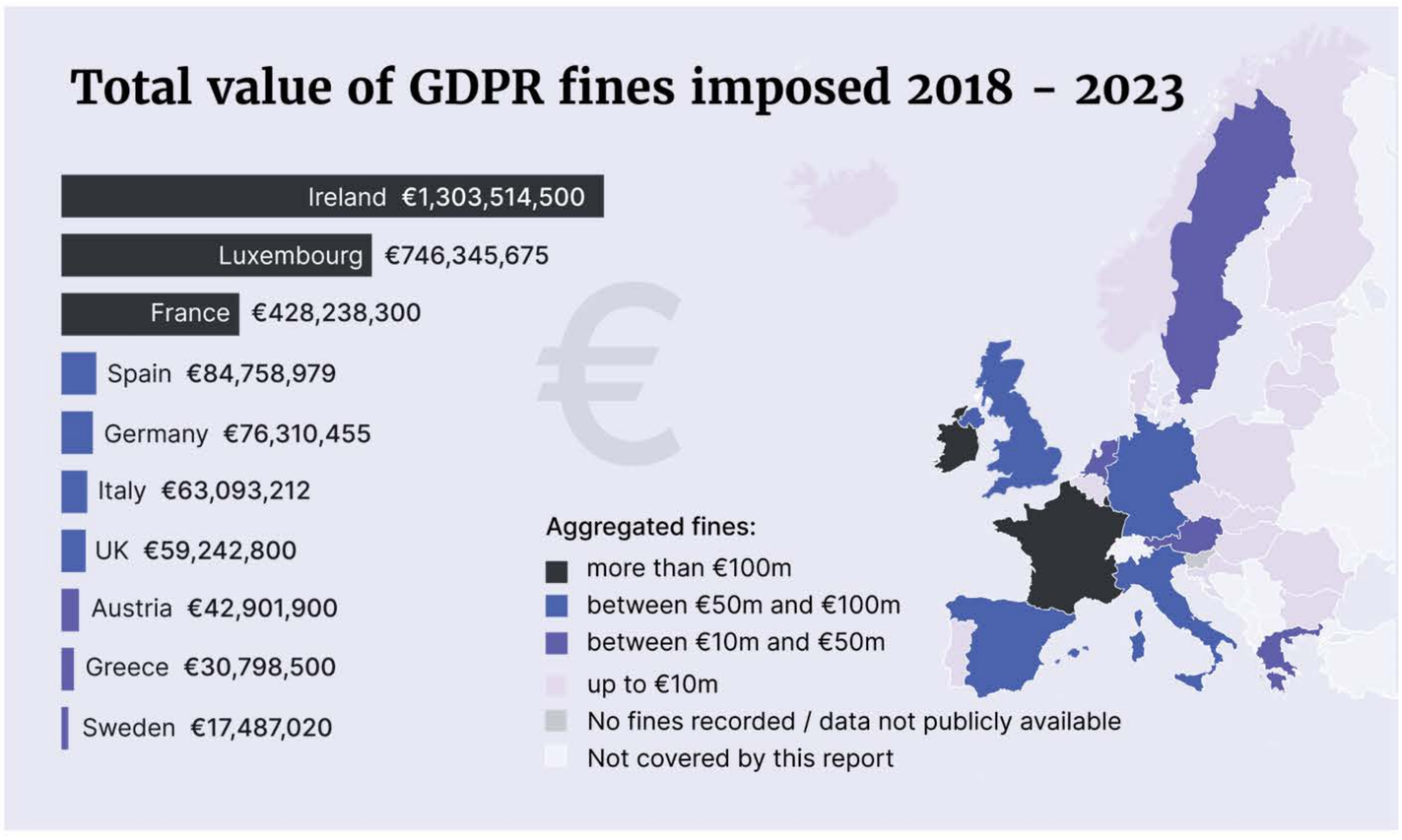
"Where does a consumer get advice on whether they have the right cover for their vehicle? I'll tell you — from the police officer who fines them and gives them six points for driving uninsured."

But regulators need to make what exists work as well as possible. For all the understandably high-profile action around car insurance, it's far from clear that regulatory intervention as it's currently being deployed will, or even can, achieve real benefits for consumers. ●

IMAGE: GETTY

In Practice

Our digital information service GRIP covers new reports and events that affect the practice of compliance and regulatory affairs. Here's a selection of key stories from **grip.globalrelay.com**



Data regulation

EU AUTHORITIES ISSUE NEARLY €3BN IN GDPR FINES

By **MARTINA LINDBERG**

European data regulators issued a record €2.92bn ($3.16bn) in fines in the 12 months from January 2022, a 168% increase from the previous year. A new report, *GDPR and Data Breach Survey: January 2023* published by law firm DLA Piper, details breaches in all EU member states as well as the UK, Norway, Iceland and Liechtenstein.

"The increase demonstrates authorities' growing confidence and willingness to impose high fines for breaches of GDPR, particularly against large technology vendors. It has also been influenced by the highly inflationary impact of the European Data Protection Board (EDPB)," the report states.

Despite the big increase in fines, the average amount of daily breach notifications was slightly lower than last year, at 300 during the past 12 months, compared to 328 in 2022. A total of around 109,000 personal data breaches were notified to regulators, a decrease on the previous total of 120,000 breaches.

The report suggests any decrease could be because "organizations' GDPR notification procedures have become more mature and more sophisticated recording of data breach notification figures by supervisory authorities".

However, the reduction in breach notifications might be owing to organizations becoming more wary of reporting them, where they know the potential risk of investigations and enforcement actions, including fines and compensation claims that could follow.

Meta in Ireland faced the biggest fine of the year, €405m ($439m). This was imposed by the Irish Data Protection Commissioner (DPC) over failure to protect children's personal data on Instagram.

That action was the first EU-wide decision on children's data protection rights.

Later in the year, the DPC fined Meta again, this time €265m ($275m) for data protection "by design and default" failings, which led to the exposure of personal details of 533 million users. Both fines are currently under appeal.

Companies in Ireland dominated the list of the year's largest fines, as well as suffering the biggest aggregated value of fines since 2018, a total of more than €1.3bn ($1.4bn).

Five of the 10 biggest GDPR fines, all issued by the DPC this year, were imposed on Ireland-based Meta.

The biggest individual fine ever, €746m ($790m), was imposed on Amazon in July 2021 by the Luxembourg data protection supervisory authority. This fine is also under appeal.

While the biggest fines were issued on companies in Ireland, the Netherlands had the most data breach notifications in total. Since May 25, 2018, the top 10 countries with the most personal data breach notifications are:

- Netherlands – 117,434
- Germany – 76,967
- UK – 49,213
- Poland – 41,751
- Denmark – 34,516
- Ireland – 29,692
- Sweden – 23,411
- Finland – 20,880
- France – 15,748
- Norway – 9,414

Lichtenstein has the lowest number of data breach notifications, with just 147 in total. Most European countries have total aggregated fines up to €10m ($10.8m).

Continuing a trend from last year, the report also showed that supervisory authorities prioritized enforcement actions in relation to breaches of the core data protection principles in Article 5.

These actions were taken for failure to comply in two areas: the lawfulness, fairness and transparency principle (Article 5(1)(a)) and the integrity and confidentiality principle (Article 5(1)(f)). ●

Climate regulation

FAIR SHARE EXEMPTION COULD EASE ANTITRUST FEARS

By **MARTIN CLOAKE**

The UK's Competition and Markets Authority (CMA) is aiming to relax antitrust safeguards to make it easier for businesses to work together on climate change initiatives.

New CMA chief executive Sarah Cardell told a forum in Scotland that the regulator would consult next month on a measure to "provide more clarity on what businesses can do".

The move comes in response to lobbying from the Glasgow Financial Alliance for Net Zero (Gfanz), a global coalition of financial institutions which aims to accelerate decarbonization. The group, which has 550 members, has voiced fears that coordinated action on climate change could leave businesses open to action over breaching competition law.

Cardell indicated that the CMA would be looking to incorporate sustainability initiatives into existing competition law exemptions. Currently there is provision for firms to enter agreements that would otherwise be seen as anti-competitive if benefits outweigh harms, and if customers receive a fair share of the benefits.

The proposal being examined would class climate change mitigation as a benefit to society that would be classified under the fair share exemption. This would, for example, address fears raised by insurers that banning underwriting firms from insuring carbon-heavy sectors would fall foul of competition rules.

The CMA became an independent watchdog when the UK left the EU and the move will be seen by some as a 'Brexit benefit'. Irritation with how EU competition law hampered moves to coordinate action for practical benefit was one of the factors raised during the Brexit debate. The European Commission has also drafted guidelines that would exempt sustainability agreements under a similar "collective benefit" definition. ●

> *"AI applications are now more advanced and embedded in operations, with nearly eight out of 10 in the later stages of development"*

Technology

FCA DATA CHIEF OUTLINES REGULATION'S ROLE IN AI

By **MARTIN CLOAKE**

Collaboration, inclusion and diversity of thought are key to developing effective regulation that will allow financial services to get the best from the opportunities offered by artificial Intelligence (AI). This was the message from the UK FCA's Chief Data, Information and Intelligence Officer, Jessica Rusu, in a speech to The Alan Turing Institute's Framework for Responsible Adoption of AI in the Financial Services Industry event.

Rusu started by acknowledging the influence of the Alan Turing Institute in "advocating for positive change and for a fairer, more equitable and accessible approach to the design and deployment of technology across the UK economy". And she emphasized: "Regulation should not deter innovation, but should rather promote fair competition, protect consumers and promote the effective functioning of markets."

Potential benefits of AI

"AI has the potential to enable firms to offer better products and services to consumers, improve operational efficiency, increase revenue and drive innovation," she continued. "All of these could lead to better outcomes for consumers, firms, financial markets, and the wider economy."

She posed the question: "Is regulation necessary for the safe, responsible and ethical use of AI? And if so, how?"

Referring to the findings of a recent survey the FCA carried out alongside the Bank of England, *Machine Learning in UK Financial Services*, Rusu reminded the audience that: "The findings show that there is broad agreement on the potential benefits of AI, with firms reporting enhanced data and analytic capabilities, operational efficiency, and better detection of things like fraud and money laundering as key positives.

"The survey also found that the use of AI in financial services is accelerating — 72% of respondent firms reported actively using or developing AI applications, with the trend expected to triple in the next three years. Firms also reported that AI applications are now more advanced and embedded in day-to-day operations, with nearly eight out of 10 in the later stages of development."

But as well as benefits, there are risks or, as Rusu preferred to put it, "novel challenges for firms and regulators". The use of AI can "amplify existing risks to consumers, as well as the safety and soundness of firms, market integrity, and financial stability".

And, she said, data from the survey showed "data bias and data representativeness were identified as the biggest risks to consumers, while a lack of AI explainability was considered the key risk for firms themselves."

Effective governance

All of which meant, said Rusu: "Effective governance and risk management is essential across the AI lifecycle, putting in place the rules, controls, and policies for a firm's use of AI. Good governance is complemented by a healthy organizational

culture, which helps cultivate an ethical and responsible environment at all stages of the AI lifecycle: from idea, to design, to testing and deployment, and to continuous evaluation of the model."

Rusu explained that, despite the risks and challenges, there wasn't a need for new regulations in this particular area, as the FCA considered the existing Senior Managers' and Certification Regime (SMCR) provided "the right framework to respond quickly to innovations, including AI".

Nonetheless, Rusu revealed that the regulator would soon be publishing a call for interest in a Synthetic Data Expert Group, hosted by the FCA, which would run for at least two years. The new group's remit would be to:

- clarify key issues in the theory and practice of synthetic data in UK financial markets;
- identify best practice as relevant to UK financial services;
- create an established and effective framework for collaboration across industry, regulators, academia and wider civil society on issues related to synthetic data;
- act as a sounding board on FCA projects involving synthetic data. ●

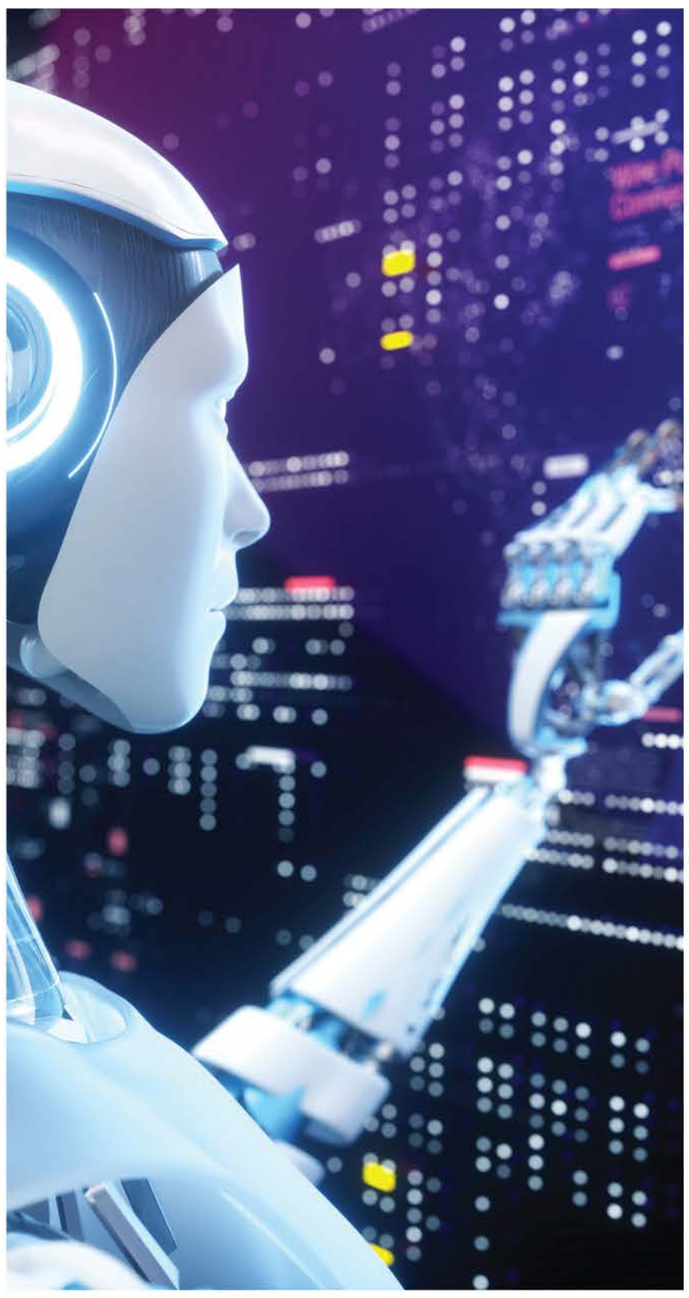


IMAGE: GETTY

> *"Digitalization means that the crime landscape is different. New fraud and money laundering tactics are emerging"*

Compliance

INCREASED APPETITE FOR COMPLIANCE PROFESSIONALS, REPORT FINDS

By **CARMEN CRACKNELL**

An incredible 99% of organizations globally say they are re-evaluating their risk appetite because of the economic environment, and that "the already-hot employment market for compliance staff is likely to get hotter still", partly owing to the growth of 'super apps' looking to hire compliance professionals.

Financial institutions, digital banking and fintech, wealth management, investment (retail), capital markets, money service businesses, crypto exchanges, and insurance were the sectors covered in a recent report from ComplyAdvantage. The survey questioned 800 c-suite and senior compliance decision-makers from across the world, including the US, Canada, UK, France, Germany, Netherlands, Hong Kong, Singapore and Australia.

Some 58% of global financial institutions say they plan to hire more compliance professionals (in the UK the figure was higher at 69%), while 59% of organizations say compliance teams are preparing for an increase in financial crime as a result of the uncertain global economic environment. Concern about investment scams or tax fraud was voiced by 41% of firms, with 31% worried about phishing. Cybersecurity was acknowledged as a pain point for 53% of firms.

The report warns that as well as professional criminals "previously legitimate actors, some of which will cross the line into financial crimes" pose regulatory threats, owing to the pressures of the current cost-of-living crisis. But while compliance is a major growth area for most businesses, 48% say that knowledge of the regulations would be a concern.

"There are clear indications of 'enforcement fatigue' in this year's survey," says Iain Armstrong, Regulatory Affairs Practice Lead at ComplyAdvantage. "More than ever, compliance officers will need to keep businesses focused on good outcomes by emphasizing the human, as opposed to financial, cost of financial crime."

Of particular note, 87% of respondents say they have seen an increase in the use in the past year of decentralized finance (DeFi) platforms to fund extremism, in particular crowdfunding sites.

"Compliance officers working for firms offering DeFi services must be aware of the emerging regulations in the cryptocurrency and crowdfunding space to ensure they have adequate, effective, scalable financial crime control solutions in place. This will include transaction monitoring rules tailored for the unique typologies and behaviors they should screen for," says Alia Mahmud, Regulatory Affairs Practice Lead, ComplyAdvantage.

Whereas heading into 2022, organizations were more concerned about China, the invasion of Ukraine means the focus has shifted to Russia, with 53% saying it has forced them to change business models and 50% resorting to asset freezing. And 46% expressed "concern" about Russia, contrasting with 37% saying the same about China.

"During the 2007-09 Great Recession, financial institutions reported a significant increase in the level of financial crime," says Vatsa Narasimha, CEO, ComplyAdvantage. "Our survey shows firms — driven by the expectation of an economic downturn — expect it to rise this year. But the

digitalization of business and transactions since 2008 —accelerated by the pandemic — means the financial crime landscape is different. With new fraud and money-laundering tactics emerging all the time, agility and investment in the latest risk detection technologies have never been more critical."

A growing regulatory focus on non-fungible tokens, stablecoins, and DeFi regulation is reflected in firms' responses, with 60% saying they plan to accept crypto as a payment method/rail in future and 59% seeking out their own crypto licenses. Virtual assets risk monitoring was identified as an area for improvement by 43%.

Last year saw an acceleration in the convergence of ransomware and cryptocurrencies, notably through Deadbolt, a group attacking network-attached storage devices and vendors. The Markets in Crypto Assets Regulation, due in the next two years, will provide clarity on the matter in European markets. The EU pledged in December last year to "protect EU citizens and the EU's financial system against money laundering and terrorist financing" by drawing up a new EU AML rulebook.

The overhaul of the EU's Anti Money Laundering (AML)/Countering the Financing of Terrorism (CFT) package will trigger an overhaul of regulation and has been described as "a tectonic shift" in the approach to fighting financial crime. The new AMLD6 directive removes loopholes in domestic legislation by harmonizing the definition of money laundering across the EU. Meanwhile, the ENABLERS Act in the US expands the definition of a financial institution for purposes of reporting suspicious transactions. ●

87%

of organizations say they have seen an increase in the use of decentralized finance platforms in the past year

US regulation

ASSISTANT ATTORNEY GENERAL SIGNALS NEW APPROACH ON SELF-DISCLOSURE

By **MARTIN CLOAKE**

"Come forward, cooperate, and remediate" was the message from US Assistant Attorney General Kenneth A Polite Jr in a recent speech to Georgetown Law School. He used the occasion to set out revisions to the Department of Justice (DoJ) Corporate Enforcement Policy, notably greater incentives for companies to self-disclose misconduct.

Observers took the speech to indicate a softening of tone from the Biden administration, which had been ramping up the 'tough on corporate crime' rhetoric. Polite said it was "directed at companies that take compliance and good corporate citizenship seriously" but, as seasoned industry observer Matt Kelly said on his Radical Compliance blog, the detail raises some challenging questions.

Polite's announcement focused on the criteria for so-called declinations, decisions to decline going ahead with prosecution. From now on, prosecutors could opt for declination " if the company can demonstrate that it has met each of the following three factors":

- The voluntary self-disclosure was made immediately upon becoming aware of the allegation of misconduct;
- At the time of the misconduct and disclosure, the company had an effective compliance program and system of internal accounting controls that enabled the identification of the misconduct and led to the voluntary self-disclosure;
- The company provided extraordinary cooperation with the department's investigation and undertook remediation.

If a criminal resolution is still appropriate, Polite said, the DoJ would, if a company voluntarily discloses misconduct, cooperates fully and provides evidence of timely and appropriate remedies, "recommend to a sentencing court, at least 50%, and up to 75% off of the low end of the US sentencing guidelines fine range, except in the case of a criminal recidivist". This is a significant shift on the previous position, which allowed for a maximum 50% reduction.

For companies that do not voluntarily disclose but which fully cooperate and provide appropriate remedies, the recommendation will be for up to a 50% reduction.

Polite was keen to stress that "a reduction of 50% will not be the new norm; but reserved for companies that truly distinguish themselves and demonstrate extraordinary cooperation and remediation". But the introduction of the concept of "extraordinary cooperation" raises an important point, one set out by Kelly on his blog — how does that differ from the DoJ's previous standard of providing 'full' cooperation?

Polite attempted to address that question in his speech, saying that factors such as quality and timing of assistance, cooperation that produces results and providing evidence that leads to additional convictions would be considered.

But, as Kelly asks: "Isn't that what companies are doing already to win credit for 'full' cooperation?"

Kelly's theory is that the DoJ is "trying to cover its Fifth Amendment behind, before a federal judge decides that these cooperation policies really turn a company's in-house investigations team into an extension of the DoJ".

To back his assumption, Kelly points to Polite's comment that "the government will not affirmatively direct a company's internal investigation, if it chooses to do one, and companies are often well positioned to know the steps they can take to best cooperate in a particular given case".

Perhaps the key message from the speech for compliance and regulation professionals, CEOs and boards was one Polite delivered in the closing section: "Our number one goal in this area — as we have repeatedly emphasized — is individual accountability. And we can hold accountable those who are criminally culpable, no matter their seniority, when companies come forward and cooperate with our investigation." ●

Bob Hawk on...

Coping with the arms race in encryption

> *"We're constantly solving problems created by the solution to the last problem we dealt with"*

Encryption is taking on ever greater importance and it is not unusual to read about important developments in the area that will lead to a significant breakthrough. I was recently sent a short news item about optical computing — a great example of solving a problem caused by not thinking the previous solution through sufficiently.

The need to encrypt data is obvious, but the data still has to be unencrypted if it's to be computed. As cloud solutions become more prevalent, individual devices are sending calculations back to the cloud servers, increasing the risk that the information can be compromised. Fully homomorphic encryption (FHE) enables computation to take place directly on encrypted data. This means if you have the key, you can send information to the cloud, get it processed and receive it back without compromising anything.

But that takes a lot of time. Optical computing works by encoding data in beams of light rather than electronic currents, using a branch of mathematics called linear algebra to massively speed up processing.

The encryption arms race

This is the encryption arms race in action. We're constantly solving problems created by the solution to the last problem we dealt with. In such situations, it is often wise to step back, take a breath and ask why a particular course of action is being taken. Too many technologists are reaching conclusions without understanding the consequences. That's a bad approach to managing risk. In essence, it means addressing a problem but creating other problems in the wake of the solution to the original problem.

Cryptography starts off being very basic. You shift the alphabet over 1, 2, 3, 4, 5 or 6 places, known as the Caesar Cipher, where, for example, a Q could represent A. Systems evolved into taking a more random approach and developing a key. This then developed into using large integers to create relationships, the basis of the most modern encryption used to protect data transfer on the internet.

Old systems die hard

Systems that originated in the late-1970s, such as Diffie-Hellman and RSA, are still is use. These have shown their sustainability and longevity, but they are now coming under attack from new developments in technology, such as quantum computers, optical computers and even computers that can solve problems using DNA processors. We went from mechanical computers, such as cash registers, to electronic computers and now we are starting to move towards molecular electronics, using our DNA and artificial neural nets to try to solve equations and problems.

Within the National Institute of Standards and Technology (NIST) there is a working group known as the Federal Information Processing Standards (FIPS) which is entering its third age, referred to as FIPS publication 140-3. This defines the latest baseline for validating the effectiveness of cryptographic hardware and software. One of the considerations is referred to as quantum resistant cryptography, which in essence means cryptographic systems that can resist attacks by quantum computers.

Why it matters in finance

Encryption is important for financial services, but the repercussions of information leaking go far wider. When you start talking about critical infrastructure protection, the implications of any breaches or failures are potentially world-ending. There are some things in life you don't want an average person to be able to reach cheaply or for free, such as quantum, optical, or DNA processors and computers.

Considering that humanity is on the verge of the realization of technologies such as quantum, optical, or DNA processors and computers, it's important to understand that science can pave a path from a mathematical model perspective. The tests are whether we have the technology to build these solutions, whether we have fully considered the consequences and, ultimately, where that might lead us. ●

IMAGE: GETTY

Bob Hawk is Senior Security Administrator at Global Relay.

What do tomorrow's markets look like?

Will they be up or down?
Can I make the best of both?

UBS

For some of life's questions you're not alone.
Together we can find an answer.

ubs.com

The value of investments may fall as well as rise and you may not get back the amount originally invested.

Grip.

Get practical insights on the latest developments in compliance and technology

Visit GRIP, Global Relay's new digital information service with daily business content on key headlines and trends in the rapidly shifting compliance landscape.

For a limited time, we're offering a free trial of our new subscription content service. Check out GRIP today:
grip.globalrelay.com

Grip. By globalRELAY