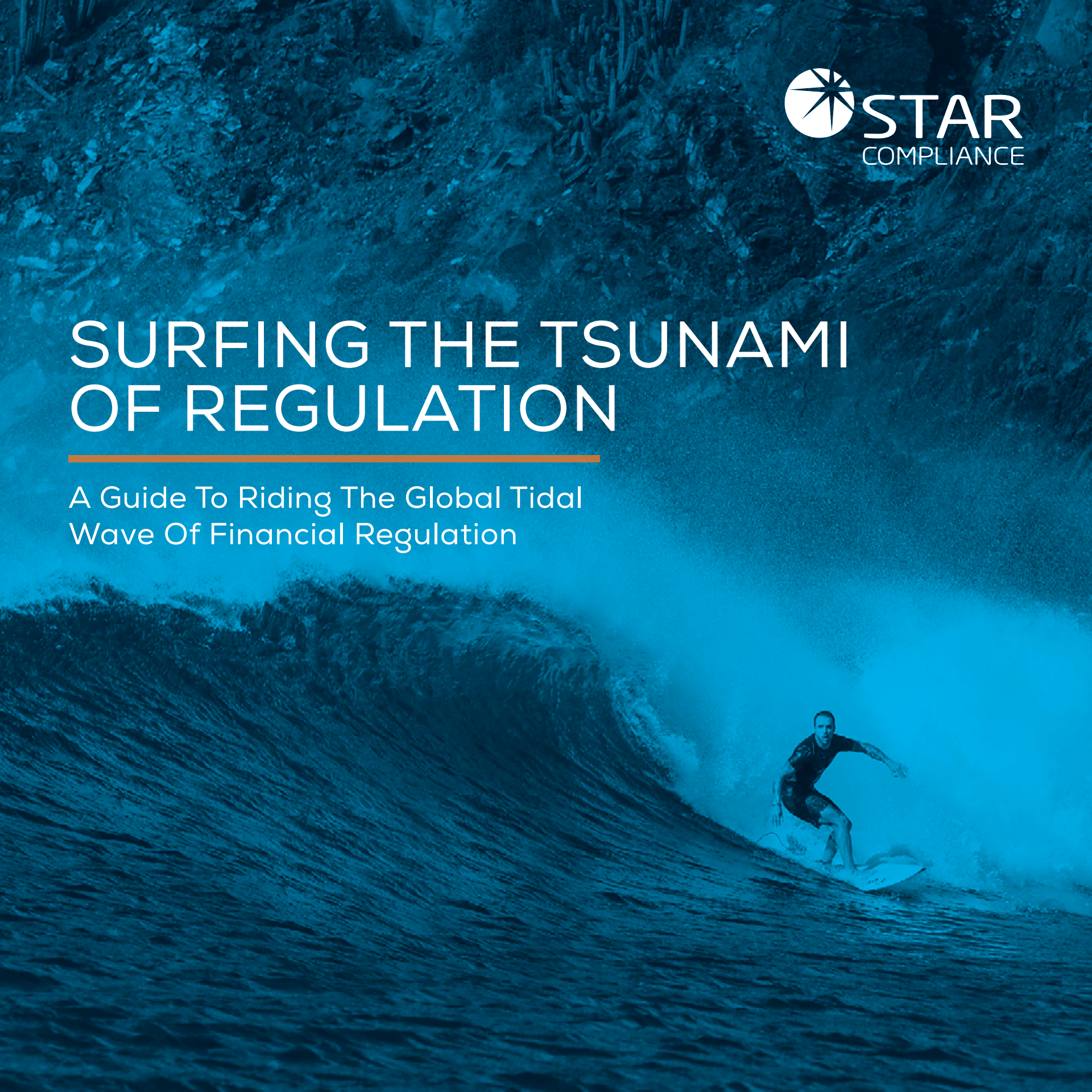


STAR COMPLIANCE

SURFING THE TSUNAMI OF REGULATION

A Guide To Riding The Global Tidal Wave Of Financial Regulation

INTRODUCTION

Created by the same tectonic shifts that cause earthquakes, tsunamis—also known as tidal waves—are the most feared of waves. Only the craziest of the world's surfers attempt to ride them. But at least they have a choice in the matter.

If you're a compliance officer, you have no choice but to paddle out every day into the ever-heightening swells of global regulation and try to guide your firm safely onto shore. The tectonic forces generating these massive regulatory waves are threefold.

The first is the global financial crisis. Though the world is 14 years out from the crash of 2008, aftershocks continue. Many countries still have not fully recovered from the dramatic economic downturn, and people and governments continue to ask questions as to how it all happened and to look for ways to prevent a recurrence. Regulatory legislation—like the UK's Senior Managers and Certification Regime, Singapore's Individual Accountability and Conduct Guidelines, and similar individual accountability regulations popping up globally—is often the answer.

Data privacy is another regulatory driver, and it's Europe that has taken that legislative lead. The GDPR turns the relationship between data processors and data subjects radically on its head. The California Consumer Privacy Act is the Golden State's answer to the GDPR and Big Tech data-privacy scandals. New York state's 23 NYCRR §500 is a response to the Target and The Home Depot data breaches of 2014.

And corruption concerns are more and more driving the passage of legislation. Brazil's Clean Company Act went into effect in 2014. France's Sapin 2 is the country's second legislative attempt to take on corruption and increase transparency. Italy's Law No. 179/2017 gives unprecedented protection to whistleblowers.

Consider this a general reference—a high-level guide—to keep yourself informed at a glance of the most relevant and potent regulation washing over the worlds of finance and compliance. And to keep your organization riding high and dry on top of it all.

THE EU: GDPR

Born out of the growing awareness that the era of Big Data meant more and more companies relying on personal data to fuel their business models, on May 25, 2018, the General Data Protection Regulation, or GDPR, became law across the European Union. Its data-privacy regime supersedes 1995's Data Protection Directive. Any company that does business with EU citizens or monitors their behavior has to comply, no matter where in the world it's based or where its work is done.

Importantly, the GDPR applies to data processors as well as data controllers. Requests for consent must be written in clear, intelligible language. It must be as easy to withdraw consent as it is to give it. Under the GDPR, all data subjects have the Right To Breach Notification, the Right To Access, the Right To Data Portability, and the Right To Be Forgotten, or data erasure. Privacy By Design is a legal requirement, and means data protection must be designed into collection and processing systems from the start.

The GDPR also creates a requirement for Data Protection Officers for controllers and processors that monitor data subjects on a large scale. The DPO can be a new or existing employee, or an external service provider, so long as he or she is qualified. Exporting data out of the EU remains banned, as it is under the DPD. Serious breaches of the new law can mean a fine of 4% of annual global turnover or €20 million, and less serious breaches a 2% fine. Data Protection Authorities have mandatory audit rights.

UPDATE

As required by Article 97 of the GDPR, the European Commission submitted its first GDPR report on June 24, 2020. This report shows that the GDPR met the majority of its objectives and proved to be flexible by supporting digital solutions during the COVID-19 crisis. Regulators today have the tools they need to enforce the GDPR and issued their largest fine of $888 million to Amazon on July 16, 2021. Moving forward, the commission will continue working with member states to ensure GDPR implementation and will report on the application in the next evaluation report, set to be completed in 2024.

For more from StarCompliance on the GDPR, read **part one** and **part two** of our in-depth blog series. For more from the EU, go to the **GDPR website**.

THE EU: MiFID 2

MiFID is a European regulation, and stands for Markets in Financial Instruments Directive. MiFID 2 and its predecessor, MiFID 1, are both primarily concerned with the welfare of the individual investor. MiFID 1 came into effect in 2007, a year before the global financial crash. Planning for MiFID 2 got underway in 2011, with the realization that MiFID 1 did not do enough to ensure the safety and resiliency of financial markets.

MiFID 2 officially sets out to:

- Ensure competition in trading and clearing.
- Ensure trading takes place on regulated platforms.
- Introduce rules on algorithmic and high-frequency trading.
- Improve the transparency and oversight of financial markets.

Regulatory scope like this means no European market goes untouched. This includes brokers, fund managers, high-frequency traders, exchanges, banks, hedge funds, and pension funds. MiFID 2 regulates equities, commodities, futures, currencies, and ETFs, as well as off-exchange markets. And anyone trading a security with a component asset listed in the EU now operates under EU jurisdiction.

MiFID 2 contains 28 Regulatory Technical Standards, or RTS, covering trade surveillance in particular: everything from microstructural issues, to data publication and access, to market data reporting, to best execution. Algorithmic trading is getting a serious relook; compliance staff will eventually need to know how their algorithmic trading engines—or algos—operate, and will have to monitor such trading in real time.

RTS 27 deals with best execution, and zeroes in on pre- and post-trade transparency across markets. Trading venues must provide quarterly reports, with details such as price, costs, speed, likelihood of execution, and settlement. RTS 28 mandates that, for every trade, firms must record class of financial instrument, venue name, and the volume of orders executed on each venue. Sixty-five data points will need to be recorded. In the end, banks and brokers must be able to prove that, whatever route through whatever exchanges and expediters they chose for a trade to travel, their customers got the best price.

UPDATE

Due to the COVID-19 crisis, the European Parliament and the Council of the European Union adopted a new directive. Directive 2021/338 impacts information requirements and transparency, criteria for ancillary investment activity, organizational requirements for investment service providers combined with exceptions to product governance requirements, and the provision of research by third parties. In the UK, Brexit went into effect Jan. 31, 2020, and the FCA distributed a consultation paper with proposed changes to UK MiFID in April 2021. In a statement on Nov. 30, 2021, the FCA confirmed changes in research in effect as of Dec. 1, 2021, and changes in best execution in effect as of March 1, 2022.

For more from StarCompliance on this massive regulation, check out our in-depth **blog on MiFID 2**. For more from the EU, visit the ESMA's **MiFID 2 website**.

ITALY: LAW NO. 179/2017

Law No. 179/2017 came into effect on Dec. 29, 2017. It's an anti-corruption law concerned primarily with protecting whistleblowers in the private sector. Initially, only whistleblowers in the public sector had explicit protections under Italian law, then those in banking and finance. Ultimately, however, it's from 2001's Decree No. 231 that all Italian anti-corruption law of note flows.

For the first time, companies could be held liable for crimes carried out on their behalf and in their interest by directors, executives, and subordinates. Crimes included money laundering, fraud, bribery, and market abuse. Companies could avoid liability if they had a compliance program in place specifically designed to prevent the misconduct that occurred, though Decree No. 231 never mandated the creation of one.

Law No. 179/2017 specifically sets out what it thinks a good whistleblower protection scheme in a company's already existing organizational and management model should look like:

- To protect a whistleblower's identity there must be more than one whistleblower channel, and at least one whistleblower channel must be computerized.
- Retaliating or discriminating against whistleblowers is strictly forbidden, and the policy against such action must be made clear in company policy.
- There must be disciplinary measures in place for those who retaliate or discriminate against whistleblowers.
- There must be disciplinary measures in place for those who intentionally file false or unsubstantiated reports of violations.

It's important to note that all of this applies to foreign companies operating in Italy, even if they don't have a branch there. For any compliance program your firm already has in place, check to make sure it complies with Decree No. 231 requirements as your starting point. For example, the definition of public official under Italian law appears to be broader than in other countries. As always, do your due diligence.

For more from StarCompliance, read our in-depth **blog on Law No. 179/2017**.

FRANCE: SAPIN 2

Sapin 2 makes it a crime to try and influence a foreign public official. This means no donations, gifts, or rewards in the hope of gaining unfair advantage. It applies to legal or natural persons, and French prosecutors can bring charges even if the crime was perpetrated outside the country. It took effect June 1, 2017, and its full title is *The Transparency, Anti-Corruption, And Economic Modernization Bill*.

Sapin 2 promotes and increases transparency by creating a national register of *representatives of interests* and gives financial-sector whistleblowers the official protection of the state. It also creates an obligation for all large companies to implement corruption-prevention plans. Any company with a workforce of more than 500 with an annual turnover that exceeds €100 million must have codified plans in place to prevent corruption. Workforce training is listed as one example of what a plan might be.

In the case of a breach, there can be formal warnings, the threat of taking penalties public, and fines: up to €1 million for legal entities and €200,000 for natural persons. Sapin 2 also introduces *deferred prosecution agreements*, also known as a *convention judiciaire d'interêt public*, or CJIP. Like with DPAs, CJIPs can be offered to defendants willing to cooperate with prosecutors as a way to avoid prosecution, with the agreement that all charges will be dropped in return for full cooperation.

In the case of a CJIP, a fine may be levied against the legal person, up to but not more than 30% of the organization's annual turnover. The company must also agree to bring its procedures for preventing and detecting corruption and influence peddling into compliance under supervision of the government. It's worth noting that under Sapin 2, companies can be targeted for prosecution simply for not instituting mandated anti-corruption practices.

For more from StarCompliance on Sapin 2, check out our **in-depth blog**. For more from the French government, visit the **official Sapin 2 webpage**.

BRAZIL: CLEAN COMPANY ACT

On Jan. 29, 2014, Law No. 12,846—The Clean Company Act—took effect. It's an anti-bribery and anti-corruption law that applies to Brazilian businesses, Brazilian foundations or associations, and foreign firms with a presence in the country. Any of these entities can be held liable for prohibited acts committed in their interest or for their benefit. To be held liable, authorities don't have to prove intent on the part of the entity or any officer of the entity, only that the act occurred.

Charges can only be brought against companies, however, not individuals. Individuals involved in wrongdoing related to any charges brought against companies under the act can be prosecuted under Brazil's existing criminal code and related Brazilian law. And that's the real point of Law No. 12,846: to encourage investigations of company wrongdoing in the hope evidence gathered will allow for individual prosecution under other Brazilian law.

Law No. 12,846 also applies to government entities: specifically, illegal acts involving Brazilian or foreign public officials. It prohibits any promises or offers that would directly or indirectly give undue advantage to a public official or third person. It also prohibits any efforts to finance, pay, or in any way subsidize the performance of a prohibited act.

Brazil's Clean Company Act also offers the ability to resolve corruption and bribery related matters via DPAs. Also known as leniency agreements, these legal mechanisms encourage firms to self-report violations, with the understanding that by doing so firms may be given credit by prosecutors. Emphasis on "may." There are no guarantees. Firms that cooperate with authorities in this manner—enter into leniency agreements—and do what's required of them could have their fines significantly reduced.

For more from StarCompliance, check out our in-depth blog on **Brazil's Clean Company Act**.

THE US: RULE 17A-4

SEC Rule 17a-4 has its regulatory origins on the data side of things, but data security rather than data privacy. Part of the Securities Exchange Act of 1934, Rule 17a-4 specifies how records created by broker-dealers must be kept, as well as how long. In 1997, it was amended to allow those records to be stored in a non-rewriteable, non-erasable electronic format. At the time, this meant DVDs and CD-ROMs.

But as technology changed, broker-dealers began asking if they could store their data on systems that used hardware in tandem with software to make data unalterable on storage media that was otherwise meant to be altered, like computer hard drives. In 2003 the SEC essentially said yes, and simply set the standards electronic storage media must meet rather than specifying a type of tech that must be used.

Per Rule 17a-4 storage must:

- Verify the quality and accuracy of the recording process.
- Serialize the original/duplicate units of storage media.
- Time-date the period of retention of the data stored.
- Be able to download data to any medium acceptable to the SEC.

Systems that use passwords, or other extrinsic security controls, are not considered unalterable and are therefore noncompliant, as are systems that just create a "fingerprint" of a record based on its content.

For help meeting Rule 17a-4, look for compliance software that takes a "save everything" approach: snapshotting every data change on every table and then saving the changes in a full history record. Look for a vendor that uses a relational database, like Microsoft SQL Server, which is designed to handle the kind of structured data generated by broker-dealers.

And when it comes to the critical issue of database backups, consider a vendor that uses WORM tape. WORM is short for write once, read many. While magnetic tape is typically known as a rewriteable medium, WORM tape uses the kind of hardware-software combination mentioned earlier to make a storage system that's verifiably unalterable and therefore automatically Rule 17a-4 compliant.

For more from StarCompliance on SEC Rule 17a-4, and specifics on how automated compliance software can help you comply, read our **in-depth blog**. For more from the SEC, visit the **SEC Rule 17a-4 webpage**.

THE US: THE CALIFORNIA CONSUMER PRIVACY ACT

AB-375 was signed on June 28, 2018. Also known as the California Consumer Privacy Act, AB-375 gives California residents ownership of their personal data, control of their personal data, and reassurance regarding the safety of that data. Specifically, Californians will now have the right to:

- Delete their data.
- Say no to the sale of their data.
- Know all the data collected on them by a business.
- Know the commercial purpose of collecting their data.
- Know the third parties with whom their data is shared.
- Know what categories of data will be collected prior to collection.

Like the GDPR, AB-375 puts the onus on companies to not just protect personal data but to be very clear about why they need it at all.

The act officially went into effect on Jan. 1, 2020. Amendments are possible and are, in fact, very likely. Big Tech may have overall supported this bill, but only because it viewed the alternative (a much more restrictive ballot initiative was in the works at the time) as far worse.

The act is enforced by the attorney general of the state of California. Under the law, the AG can fine companies that don't properly protect personal data. Businesses that must comply with the act include:

- Those that earn $50 million a year or more in revenue.
- Those that sell 100,000 consumer records each year.
- Those that derive 50% of their revenue by selling personal data.
- Those that collect or sell any Californian's personal data, no matter where in the world that business is located.

UPDATE

On March 15, 2021, then-California Attorney General Xavier Becerra announced additions to the CCPA to strengthen consumer data privacy regulation. New regulations prohibit companies from forcing customers to take unnecessary steps to opt out of the sale of their personal information and present a standard and recognizable opt-out icon that businesses can use on their websites to ensure that customers are aware of their rights. In its first year, the top industries impacted by CCPA-related filings were healthcare and health services, financial services, and technology (communication), respectively.

For more from Star on the California Consumer Privacy Act, check out our **overview blog** on the subject as well as our **regulatory update story**. For more from the state of California, visit the **law's official website**.

THE US: 23 NYCRR §500

In the works since the Target and Home Depot breaches of 2014, 23 NYCRR §500 is a creation of the New York Department of Financial Services. It was designed to "promote the protection of customer information as well as the information technology systems of regulated entities." 23 NYCRR §500 officially went into effect March 1, 2017, but had a series of rolling deadlines. The next important one was Sept. 1, 2018. By then, financial institutions must have begun:

- Keeping an audit trail of all financial transactions.
- Keeping that information for at least five years.

Further, regulated data:

- Must now be encrypted.
- Must now be erased when it's no longer needed.

Banks must also now keep an audit trail of "security events" for three years. Previously, banks were only required to do so for 30-60 days. The audit trail and information retention requirements address the concern that, if critical customer information is stolen or destroyed, it can easily be recovered. The encryption requirements get at the notion that, if data is stolen, it can't be used by the thieves as quickly or as easily. All this for the benefit of the consumer. The individual. For the moment, DFS hasn't finalized how it will penalize financial institutions that don't comply with the new law. That will change.

UPDATE

Although 23 NYCRR §50 has not been updated, the New York Department of Financial Services (DFS) has released updated FAQs to ensure the regulation's clarity. Recent penalties imposed by DFS have also shed light on what fines organizations could expect if they do not meet the requirements of this cybersecurity regulation. For example, DFS imposed a $1.5 million penalty on Residential Mortgage Services Inc. for not completing a comprehensive cybersecurity risk assessment and not fully investigating a potential data breach, among other violations.

For more from StarCompliance on 23 NYCRR §500, read our **in-depth blog post on the subject**.

THE US: PROPOSED CHANGES TO RULE 10B5-1

The Securities and Exchange Commission adopted Rule 10b5-1 in 2000 to allow insiders to outline the dates, formulas, or conditions of trading decisions in formal plans to mitigate the risk of MNPI influence. Though Rule 10b5-1 plans have been used frequently by insiders to sell and by companies to repurchase securities since the rule's adoption, detractors have questioned the flexibility the rule offers to insiders conducting transactions for several years.

The SEC included Rule 10b5-1 in its rulemaking agenda for spring 2021, and SEC Chairman Gary Gensler outlined these four primary areas of concern:

- No cooling-off period before the first trade
- No limit on when Rule 10b5-1 plans can be canceled
- No public disclosure regarding Rule 10b5 1 plans
- No limit on the number of Rule 10b5-1 plans that can be adopted

Gensler expressed concerns that the lack of a cooling-off period, allowing insiders to begin trading immediately after formalizing their trading plans, could leave too much room for bad actors to carry out insider trades. He's proposed a four- to six-month time frame for prohibiting trades. He has also suggested tighter governance over how a plan can be canceled, limits on how many plans an insider can adopt at one time, and mandatory disclosures for the adoption, modification, and terms of 10b5-1 plans. The SEC has taken no concrete steps to reform the rule based on these concerns, but changes are likely on the horizon.

For more from StarCompliance, check out our **in-depth blog post on the changes to Rule 10b5-1**. For more details on the plan, **read this article** from the Harvard Law School Forum on Corporate Governance.

THE UK: SMCR

The SMCR, or Senior Managers and Certification Regime, went into effect for all UK banks, building societies, credit unions, branches of foreign banks operating in the UK, and the largest investment firms on March 7, 2016. By replacing the Approved Persons Regime, or APR, for solo-regulated firms on Dec. 9, 2019, SMCR aims to strengthen consumer protection and market integrity with accountability for individual employees. The Conduct Rules set minimum standards for individual behavior, and will apply to nearly all employees. The most senior people will need FCA approval before starting their roles. This is the Senior Managers Regime.

The Certification Regime will apply to employees who could cause significant harm to firms or customers, and firms must confirm these individuals are fit to perform their roles. All FSMA authorized firms will have to align with branches of non-UK firms with permission to carry out regulated activities in the UK.

The SMCR will extend in proportion to the size of the firm. Firms in the Core Tier must comply with the more basic requirements. Enhanced Requirements will apply to firms whose size, complexity, and impact on consumers and/or markets warrants more attention. Limited Scope firms will be exempt from some of the SMCR baseline requirements. The FCA's SMCR Guide For FCA Solo-Regulated Firms and the FCA's step-by-step, online firm-checker tool describe which scope applies.

UPDATE

As of now, SMCR does not apply to recognised investment exchanges (RIEs), credit rating agencies (CRAs), or payments and e-money firms. Because these entities are not authorized under FMSA, the FCA has no jurisdiction, but that might soon change. The FCA's 2020/21 Perimeter Report published in October 2021 shows that the FCA believes extending a similar SMCR to these entities would enhance their internal accountability and governance, promote market integrity, and improve consistency in regulatory supervision of individuals to mitigate the risk of consumer harm. The Treasury is currently considering a parallel SMCR for financial market infrastructures (FMIs) that would include RIEs.

The FCA has also made it clear that provisions in the existing SMCR extend beyond the office. Between December 2020 and April 2021, four financial service workers had enforcement actions brought against them for nonfinancial misconduct outside the workplace. Each case focused on how the individual's personal conduct impacted their integrity and reputation and seriously called into question their fitness and propriety for work in financial services.

For information on how FCA guidance has changed as relates to COVID-19 for solo-regulated firms, check out this **StarCompliance blog on the subject**. Here's our **original StarCompliance blog on the SMCR**. For more from the FCA in general, go to the **SMCR webpage**.

TWIN PEAKS

Twin Peaks is less a new regulation than a new regulatory model. Relatively new, anyway. In 1995, Dr. Michael Taylor, a Bank of England official, devised Twin Peaks as an overhaul of the UK's financial regulatory system. It called for twin regulatory-power centers, or twin peaks. The prudential regulation peak would be responsible for ensuring a safe and stable financial system and preventing financial crises. The good conduct peak would be responsible for safeguarding consumers and ensuring proper market conduct.

Australia adopted the model first, in 1997. The Netherlands in 2002. The UK only got around to adopting its own version in 2013. In April 2018, South Africa's own twin-peaks system came online. A defining feature of the model is that power should be shared equally. Each peak has a clearly defined regulatory remit, and there should be no scenario in which one peak can dominate the other. In the more traditional setup, a single regulator is responsible for keeping tabs on everyone and everything.

The other defining feature is the inclusion of all financial institutions under the regulatory umbrella of the prudential authority, a significant change from the old sectoral model. In developing Twin Peaks, Dr. Taylor recognized that the line between banks and other institutions—like insurers—had become increasingly blurred, and that more financial institutions needed to be viewed as systemically important.

Only two countries have had a twin-peaks regulatory system in place during a major financial crisis: Australia and the Netherlands. Out of the G20 nations, Australia's financial sector performed well both during and after the crash. Not so much the Netherlands. When all was said and done, foreign claims on Dutch banks amounted to 300% of GDP. Australia's record under Twin Peaks isn't perfect, however. In 2000, one large insurer nearly went under and in 2001 another went under completely.

UPDATE

Twin Peaks is a "trending" regulatory model. That's not something you hear often. Its latest incarnation is in South Africa. Read more about it **here**.

THE UK: BREXIT

The UK officially left the EU on Jan. 31, 2020. Despite efforts between the UK and the EU to come to an equivalence deal enabling financial service institutions and employees to traverse borders freely, the two parties have so far failed to reach a permanent solution.

In the absence of such a formal arrangement, a memorandum of understanding tentatively manages the exchange of financial services and supports a degree of regulatory cooperation.

Hopes for striking a deal in the near term are slim, according to David Frost, the UK Brexit minister, who said that the UK government is working under the assumption that it is "unlikely to get extensive equivalence [on financial services] from the EU in the next year or two."

As a result, the US recently overtook the EU as the leading market for financial service exports.

For more information from StarCompliance, check out our blog post on how to prepare for Brexit's impact.

For some analysis on how the financial services sector contributes to the UK economy and how Brexit may affect that contribution, check out this Dec. 8, 2021, **research briefing** from the British House of Commons.

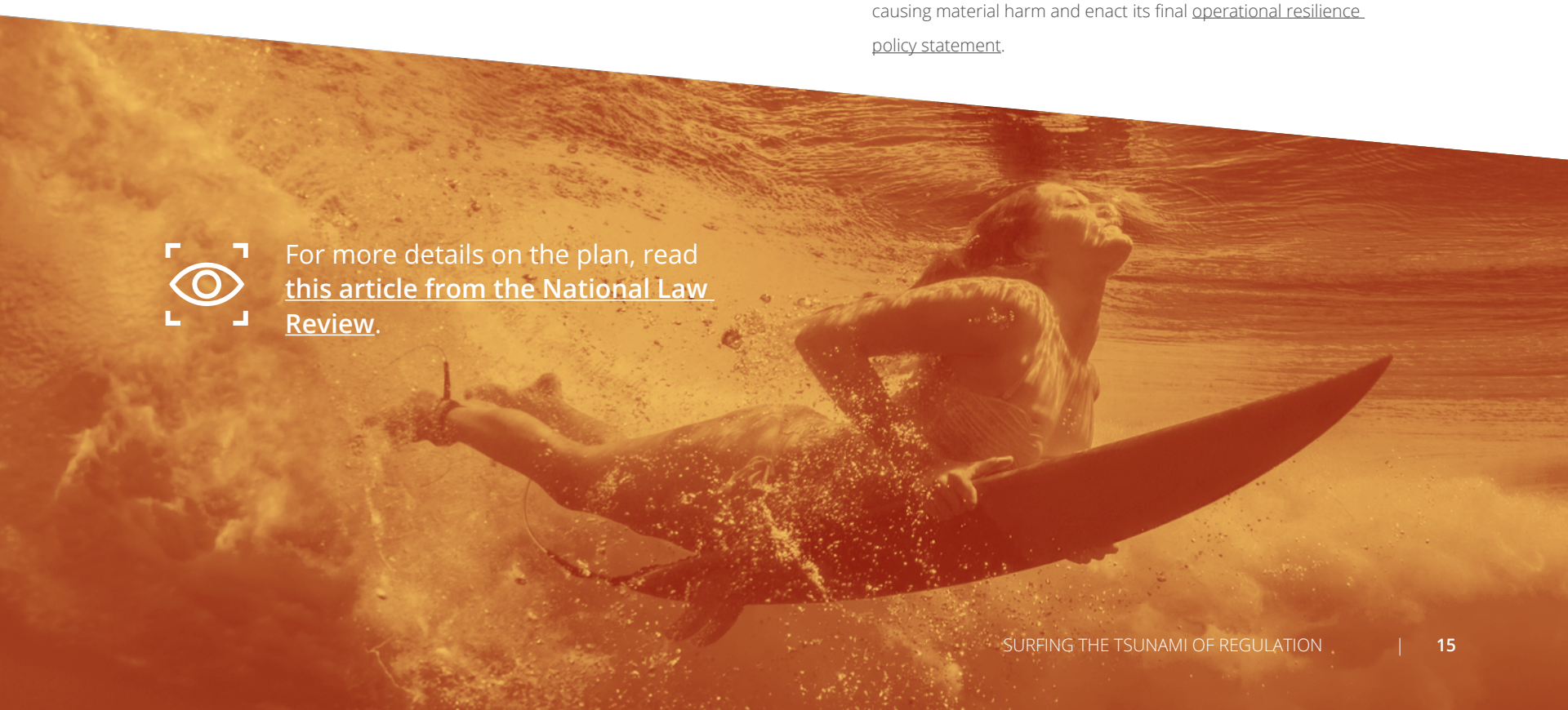
THE UK: FCA BUSINESS PLAN 2021/2022

The UK's Financial Conduct Authority published its new business plan in July 2021. The plan, which is an indicator of what can be expected from the regulator in the coming years, highlights a focus on transformation and greater accountability along with several FCA priorities.

When it comes to transformation, the plan acknowledges the quickly changing landscape of financial services in response to widespread digitization, Brexit, and other global forces. It outlines the FCA's intent to incorporate more data and technology into decision-making, become more assertive and test the limits of its powers, and grow more adaptive by adjusting to evolving consumer preferences, markets, services, and products.

The plan prioritizes three primary focus areas:

- **Consumers:** The FCA wants to protect consumers from poor advice and risky investments as their financial behaviors have changed drastically in response to financial hardship and historically low interest rates during the pandemic. The plan outlines the intent to enable consumers to make informed financial decisions, ensure consumer credit markets operate properly, and carry out other consumer-focused initiatives.
- **Wholesale markets:** Market integrity will remain an FCA focus as the regulator acknowledges the impact of wholesale markets on the economy. It aims for a smooth transition away from LIBOR to encourage trust and participation, reduce financial crime, prevent market abuse, and provide investors with fair value products.
- **Cross-market:** The FCA also expanded its focus with a cross-market lens and plans to address broader issues such as proactive monitoring to reduce fraud. It also plans to strengthen data-driven monitoring and targeting intervention to prevent firms from causing material harm and enact its final operational resilience policy statement.



For more details on the plan, read **this article from the National Law Review**.

THE UK:
FCA REMOTE/HYBRID WORKING EXPECTATIONS FOR FIRMS

Many firms have already adapted their systems and controls for remote or hybrid work environments in response to the ongoing pandemic. As many will likely continue such working conditions well into the future, the Financial Conduct Authority has set forth expectations applying to already registered firms, firms applying to be regulated, or firms planning further applications.

In a high-level overview, the FCA requires regulated firms to prove that their lack of a centralized physical location or remote/hybrid working arrangements do not or are unlikely to impact a number of situations specified by the FCA, including the accuracy of the Financial Services Register and the risk of financial crime.

Firms must also prove that they've done satisfactory planning encompassing another list of checkpoints provided by the FCA, including appropriate and maintainable governance and oversight from senior managers under the SMCR and proper recordkeeping procedures in a remote/hybrid setting.

The FCA also expects open and cooperative engagement around remote/hybrid working arrangements. Among other communication expectations, the FCA states that firms must ensure employees understand that regulators can visit any location where work is performed, including employees' homes, for regulatory purposes. The FCA also requires full access to firms' sites, records, and employees.

For more information on the FCA's expectations for remote/hybrid work, check out our **blog post on the topic** or see the **FCA's website** for detailed guidelines.

THE EU: REPUBLIC OF IRELAND

In accordance with the international Financial Stability Board's recommendations for national authorities to define key responsibilities, hold individuals accountable, and assess the suitability for individuals in charge of key responsibilities, the Central Bank of Ireland has advocated for individual accountability with two key regulations: the Fitness and Probity Regime and the Administrative Sanctions Procedure.

The Fitness and Probity Regime assigns first-line responsibility to firms and management for assessing individuals for suitability in their roles, both at the time of hire and on an ongoing basis thereafter, and for ensuring the effective operation of the regime. The Administrative Sanctions Procedure is the means by which the Central Bank investigates breaches and determines sanctions for firms and individuals.

Through ASP, the Central Bank has conducted 122 enforcement actions totaling more than €64 million in monetary penalties. For example, in 2017, the Central Bank fined Merrion Stockbrokers €200,000 for inadequate compliance systems and controls under Fitness and Probity Standards for senior and influential individuals.

However, enforcement for individuals remains challenging. The Central Bank has proposed a list of reforms known as the Individual Accountability Framework to promote a culture of greater individual accountability. The Central Bank outlines these four elements of the proposal:

- Enforceable Conduct Standards to outline the behavior the Central Bank expects of regulated firms and the individuals working within them
- A Senior Executive Accountability Regime, or "SEAR," to ensure clearer accountability by placing obligations on firms and their senior members to clearly set out where responsibility and decision-making lie for the business
- Further enhancements to the current F&P Regime to strengthen the onus on firms to proactively assess individuals in controlled functions on an ongoing basis, including giving the ability to investigate people who performed controlled function roles in the past
- A unified enforcement process, which would apply to all breaches by firms or individuals of financial services legislation and recommend that the hurdle of participation be removed such that the Central Bank could directly pursue individuals for misconduct under the Administrative Sanctions Procedure

For more on Ireland's Individual Accountability Framework, check out this article on the Central Bank's website.

AUSTRALIA: BEAR

Regulations calling for more accountability from firms and their senior managers are on the rise globally. In the UK it's the Senior Managers and Certification Regime, or SMCR. In Australia, it's the Banking Executive Accountability Regime, or BEAR. The SMCR was part of the UK's answer to what was perceived to be a broken banking culture. The same kind of thinking drove the implementation of BEAR. BEAR is part of Australia's Banking Act 1959, and was added to the law in February 2018. It's administered by the Australian Prudential Regulation Authority, or APRA. Accountability for large authorized deposit-taking institutions, or ADIs, began July 2018, and for small- and medium-sized ADIs in July 2019. Per the APRA information paper outlining its implementation, BEAR establishes "clear and heightened expectations of accountability for authorized deposit-taking institutions, their directors, and senior executives, and set out clear consequences in the event of a material failure to meet those expectations." The paper also stresses that the APRA expects ADIs to "take ownership" of BEAR compliance through "genuine reflection and consideration of mechanisms to improve governance and accountability."

UPDATE

The Australian government, in consultation with the Royal Banking Commission, is proposing to extend BEAR beyond the current scope of ADIs to include all entities regulated by APRA. This expansion is codified in new legislation dubbed Financial Accountability Regime Bill 2021, or FAR. Modeled after the UK's dually regulated SMCR, FAR will be jointly administered by APRA and the Australian Securities and Investments Commission (ASIC). If passed, FAR would replace BEAR with similar, but enhanced, responsibilities for applicable entities and individuals.

Key differences include:

- Expansion of regulation to all APRA-regulated entities
- Enhanced investigatory and enforcement powers for APRA and ASIC coupled with significantly higher financial penalties for noncompliant entities
- Expanded definitions and obligations of accountable persons

For a list of what BEAR requires of its adherents, read StarCompliance's blog on the subject and access APRA guidance for BEAR here.

HONG KONG: FMCC

On Nov. 17, 2018, changes announced in 2017 to the Fund Manager Code of Conduct, or FMCC, went into effect. The Securities and Futures Commission, or SFC, regulates the Hong Kong Stock Exchange and is overseeing the changes, which are aimed at asset managers licensed and registered in Hong Kong. The new regime works to increase transparency in financial markets and reduce risk, and in so doing better align the city's investment industry overall with international standards. Here are the changes:

- Fund managers responsible for the overall operation of a fund will be affected. The fund manager is responsible for the overall operation of the fund if the senior management make up a majority of the fund's board, representatives of the fund manager constitute a majority of the fund's board, or the fund manager is responsible for day-to-day management of the fund.
- Counterparty risk is a danger to both parties and is a source of worry to regulators, who want to make sure the possibility of default is given due consideration. To this end, under the revised FMCC the SFC expects fund managers to have collateral valuation and management policy, haircut policy, and cash collateral reinvestment policy in place to manage counterparty risk.
- Another source of risk regulators worry about is liquidity: how easily and how likely an asset can be sold at its current price. As such, methodologies should be appropriate to the nature, liquidity profile, and asset-liability management of each fund, and managers should perform liquidity stress testing on their funds on an ongoing basis.
- Fund managers should disclose the expected maximum level of leverage they've employed on behalf of their funds. Here, the SFC is addressing the risk of being overleveraged, which is dangerous to individual funds and also systemically.
- Side-pocket accounts contain hard-to-value assets, like vintage cars or paintings. To mitigate the risk associated with these illiquid assets, fund managers must have valuation policies in place, risk management competency, and proper control measures.
- As regards independent fund valuation, fund managers must adhere to a set of principles published by the International Organization of Securities Commissions, which include appointing a qualified third party to be involved in the valuation process.

For more from StarCompliance on the FMCC, check out our **in-depth blog on the subject**. You can access the SFC's own guidance on the FMCC **here**.

SINGAPORE: IAC

In September 2021, the Monetary Authority of Singapore's (MAS) Guidelines on Individual Accountability and Conduct went into effect to promote ethical business practices and vigorous risk management.

The IAC guidance follows a global movement toward greater financial institution and senior manager accountability. Preceded by the UK's Senior Managers and Certification Regime, Hong Kong's Manager-In-Charge regime, and Australia's Banking Executive Accountability Regime, the MAS Guidelines on IAC enforce the idea that compliance begins with accountability among senior managers and other FI leaders.

The guidelines list five accountability and conduct outcomes FIs in the region must aim to achieve:

- **Outcome 1:** Senior managers responsible for managing and conducting the FI's core functions are clearly identified.
- **Outcome 2:** Senior managers are fit and proper for their roles, and held responsible for the actions of their employees and the conduct of the business under their purview.
- **Outcome 3:** The FI's governance framework supports senior managers' performance of their roles and responsibilities, with a clear and transparent management structure and reporting relationships.
- **Outcome 4:** Material risk personnel are fit and proper for their roles, and subject to effective risk governance, and appropriate incentive structures and standards of conduct.
- **Outcome 5:** The FI has a framework that promotes and sustains among all employees the desired conduct.

The ease or difficulty of implementing these guidelines will vary greatly among FIs in the region and depend heavily on the maturity of compliance programs. But all compliance teams will inevitably face an increased scope of responsibility under the new regulation. In accordance with the guidelines, compliance teams are now responsible for identifying senior managers with responsibilities for core management functions, assessing each senior manager before hiring and on an ongoing basis to ensure they remain fit for the job, and holding senior managers accountable for their actions and those of their employees.

Beyond senior management, compliance teams must also identify material risk personnel, i.e., those who have decision-making authority to significantly impact the safety and soundness of an institution, its customers, or its stakeholders. FIs must also ensure regular competency training and develop incentive structures for material risk personnel to encourage conduct in alignment with the five outcomes.

What's more, FIs must establish a framework for communicating the proper standards of conduct expected of all employees under the MAS Guidelines on IAC. Compliance teams must oversee and report on any matters relating to conduct and have clear strategies to escalate concerns to the board and senior management and to share relevant information with the proper stakeholders.

For more from StarCompliance on this regulation, check out our in-depth blog post on the MAS Guidelines on IAC. For more from the Monetary Authority of Singapore, see the MAS guidelines document.

INVESTOR INTEREST IN SPACS

Special purpose acquisition company (SPAC) IPOs increased exponentially in 2020 and 2021, outpacing previous years by about 500%. The pace slowed in second-quarter 2021 in response to an SEC announcement in consideration of new SPAC IPO guidance, expressing concerns about the potential of these transactions to create issues with accounting and reporting. SEC Chairman Gary Gensler noted that SPAC IPOs incentivize SPACs to land a merger deal "even if it's not a particularly great merger," which could potentially harm investors.

In July 2021, the SEC announced its first enforcement against one SPAC, its sponsors and CEO, and the proposed merger target and its CEO and founder. Still, regulators in Asia and the EU have enacted rules to allow SPAC issuance in their jurisdictions, and deal activity is likely to continue in the US. With further regulation on the horizon and continued SPAC activity, firms will be wise to consider the associated risks carefully.

Recent statements and actions from global regulators highlight several areas where firms should aim their focus:

- Firms should be wary of any misaligned incentives and interests of SPAC sponsors and shareholders.
- Sponsors must provide adequate disclosure about potential acquisition targets to shareholders and conduct appropriate due diligence.
- Any known potential risks that relate to the target company must be clearly articulated, and retail investors must have access to sponsors' suitability analyses

For more information on new SPAC regulations and what they'll mean for compliance teams, read our article on the topic in *International Banker*.

POWERFUL WAVES. POWERFUL CROWDS.

When it comes to regulatory compliance, there's a lot to manage and a lot to keep up with. Help can be found in a variety of places.

Staying abreast of changes and shifts in thinking through the major financial newspapers and other major-media financial outlets is an obvious one. Many law firms, consulting firms, enterprise financial institutions, and compliance specialty firms, like StarCompliance, offer blog sections on their websites that can be relied upon to help keep you informed. And guides like this one can give you a crucial high-level view of the regulatory landscape, with the option of zooming in for a closer look through links out to complementary resources.

Technology, of course, should always be top of mind when you're looking for help managing fast-changing, fast-moving information flows. Automated compliance software is becoming more sophisticated practically by the week, as developers constantly refine their products based on client feedback, and then use that knowledge to sharpen platform performance for everyone's benefit.

It's perhaps that power of the crowd then, however and wherever you find it, that will offer the most help of all when it comes to surfing this tsunami of global regulation safely, successfully, and maybe even gracefully, onto shore.