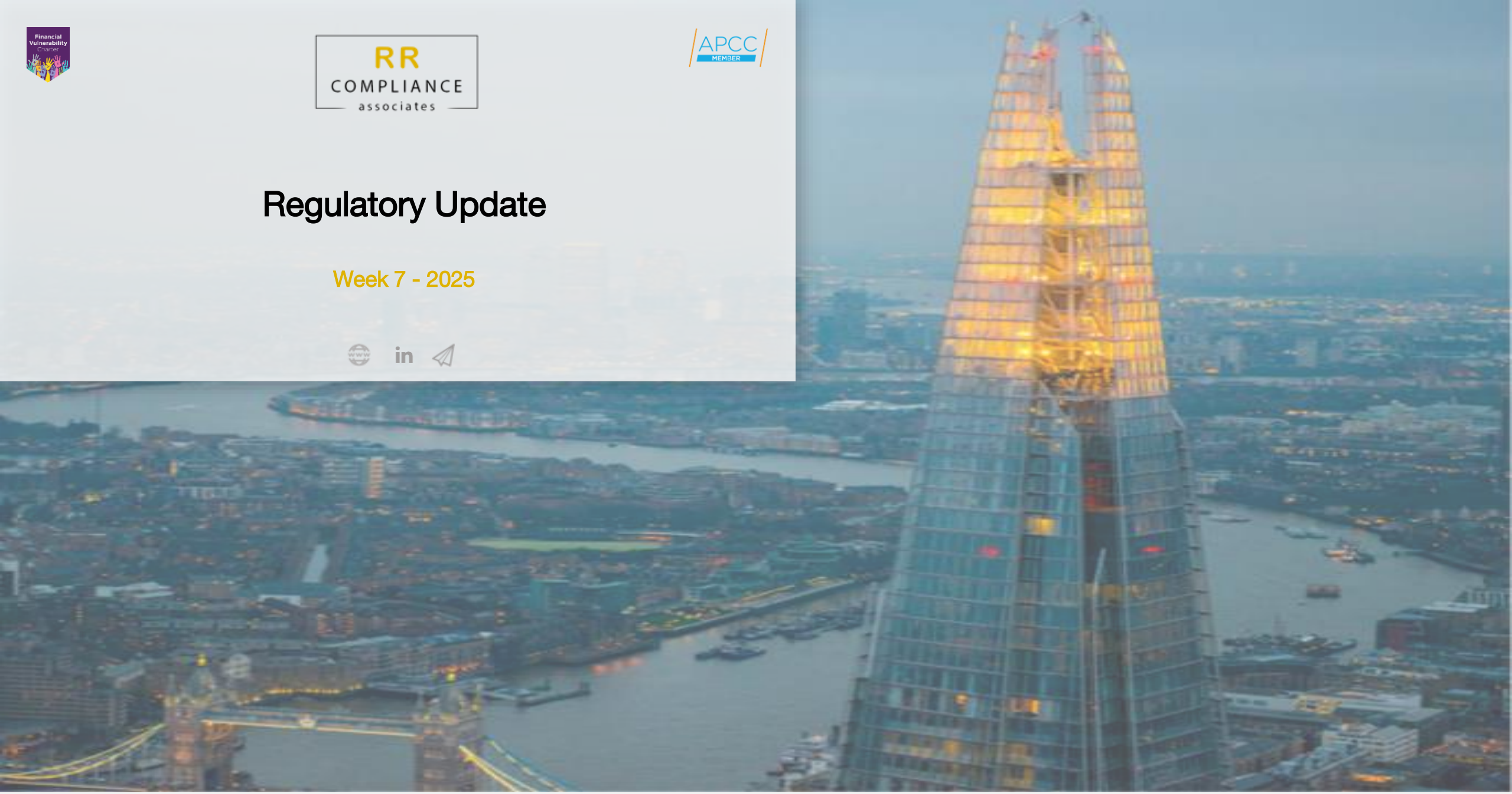
Regulatory Update

Week 7 - 2025



FEBRUARY 2025

M	T	W	T	F	S	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

Week 7

REGUALTORY UPDATES

CHECK OUT MORE RESOURCES& DESK-AID

HAVE A QUESTION? GET IN TOUCH!

Regulatory Updates – FCA (General).

Update	Summary	Action for firms
FCA publication – quarterly financial promotions data Applies to: All firms,	The Financial Conduct Authority (FCA) has recently published its Q4 2024 financial promotions data, revealing a significant escalation in regulatory interventions. Between October and December 2024, the FCA mandated the amendment or withdrawal of 3,697 promotions from authorised firms, a notable increase from the 1,004 interventions in the same quarter of the previous year. Concurrently, the FCA issued 584 alerts concerning unauthorised firms and individuals, with 11% related to clone scams—fraudsters impersonating legitimate firms to deceive consumers. This marks a decrease from the 793 alerts in Q4 2023, where 6% pertained to clone scams. The data indicates a substantial rise in the FCA's proactive monitoring efforts, which accounted for 72% of the 1,358 financial promotions reviewed in Q4 2024, up from 31% in the same period the previous year.	**Action to Take:** • Given the FCA's proactive stance, firms should consider engaging with compliance experts to navigate the evolving regulatory landscape effectively. Regular audits of promotional content, comprehensive staff training, and the implementation of robust compliance frameworks are essential steps to mitigate the risk of regulatory breaches. • Review publication here.

Regulatory Updates – FCA (General).

Update	Summary	Action for firms
Economic Crime and Corporate Transparency Act 2023 – Failure to Prevent Fraud Offence Applies to: All firms	The Financial Conduct Authority (FCA) has intensified its efforts against misleading financial promotions, as evidenced by its recent actions. In 2024, the FCA mandated the amendment or withdrawal of nearly 20,000 financial promotions, almost doubling the interventions from the previous year. A significant portion of these interventions targeted claims management companies (CMCs), with 9,197 promotions withdrawn in 2024. Many of these promotions pertained to housing disrepair and motor finance claims, often directed at vulnerable consumers. The FCA has also expressed concerns about the role of social media influencers, or 'finfluencers', in promoting financial products. In 2024, the FCA interviewed 20 individuals under caution for illegally promoting financial services products. This action underscores the regulator's commitment to ensuring that financial promotions are clear, fair, and not misleading.	**Action to Take:** • To further strengthen the oversight of financial promotions, the FCA has introduced the Section 21 Gateway. This new requirement mandates that firms obtain FCA permission before approving promotions for unauthorised persons, ensuring that only qualified entities can endorse financial advertisements. • Review publication here.

Regulatory Updates – FCA (General).

Update	Summary	Action for firms
ICO publication – 'Consent to pay' models Applies to: FinTech – gamified platforms	On 23 January 2025, the UK's Information Commissioner's Office (ICO) issued guidance on "consent or pay" business models, clarifying how organisations can implement these models in compliance with the UK's General Data Protection Regulation (UK GDPR) and the Privacy and Electronic Communications Regulations (PECR). In a "consent or pay" model, users are given a choice: either consent to the use of their personal data for personalised advertising to access a service for free or pay a fee to access the service without such data usage. The ICO's guidance confirms that such models can be lawful, provided that the consent obtained is "freely given," specific, informed, and unambiguous, and that users can easily withdraw consent at any time. Organisations considering or currently employing "consent or pay" models should conduct thorough assessments to ensure compliance with data protection laws. This includes evaluating potential power imbalances, setting appropriate fees, ensuring service equivalence, and presenting options transparently. Documenting these assessments is crucial to demonstrate compliance with the UK GDPR and PECR.	**Action to Take:** • Read the ICO guidance here.

Update	Summary	Action for firms
Jurisdiction clause takes precedence over arbitration provision in reinsurance dispute Applies to: All firms	In December 2024, the UK's Information Commissioner's Office (ICO) published its response to an extensive consultation on the application of the UK General Data Protection Regulation (UK GDPR) to generative artificial intelligence (GenAI). This consultation, initiated in January 2024, addressed key areas such as the lawful basis for web scraping, purpose limitation, data accuracy, individual rights, and controllership within the GenAI supply chain. The ICO's response maintains its original positions on purpose limitation, accuracy, and controllership. Notably, it reaffirms that legitimate interest is likely the only lawful basis for collecting data through web scraping to train AI models. However, developers must meet stringent criteria, including demonstrating clear and specific legitimate interests, ensuring necessity, and conducting a balancing test to weigh their interests against individuals' rights. The ICO emphasizes that transparency is crucial; without clear communication about data collection and usage, it becomes challenging for individuals to exercise their rights, thereby complicating the reliance on legitimate interest as a lawful basis. The ICO also addresses misconceptions, clarifying that data protection laws apply to the processing of personal data, even if such processing is incidental or unintentional. It warns against assuming that common practices equate to meeting individuals' reasonable expectations, especially concerning the novel use of personal data in training GenAI models. Additionally, the ICO distinguishes between "personally identifiable information" and the broader legal definition of "personal data," advising organizations to align their compliance efforts accordingly.	**Action to Take:** • Read further guidance here.

Regulatory Updates – FCA (General).

Update	Summary	Action for firms
ICO Fine Applies to: All firms	On 22 January 2025, the Information Commissioner's Office (ICO) announced a £200,000 fine against ESL Consultancy Services Ltd (ESL), a company based in West Sussex, for orchestrating unlawful loan promotion text messages sent to individuals without their consent. The ICO's investigation revealed that between September 2022 and December 2023, ESL collaborated with Taipan Trading Ltd (TTL), an affiliate marketer and lead generator, to disseminate these unsolicited messages. TTL employed 459 different telephone numbers, capable of sending up to 546,000 text messages daily, resulting in nearly 38,000. Evidence indicated that ESL was aware of the legal requirements for direct marketing and the ICO's role in enforcing these laws. Despite this, ESL proceeded with the campaign, attempting to conceal the identity of the message sender by using unregistered SIM cards. Additionally, ESL altered TTL's due diligence form before submitting it to the Financial Conduct Authority, removing potentially unfavourable information. This case underscores the ICO's dedication to enforcing data protection laws and serves as a reminder to businesses about the importance of obtaining valid consent before engaging in direct marketing activities.	**Action Required:** • Read the ICO publication here.

Update	Summary	Action for firms
ICO – Fee increase Applies to: All firms	In January 2025, the UK government released its response to the consultation on proposed changes to the data protection fee regime, which funds the Information Commissioner's Office (ICO). After reviewing 103 responses from various stakeholders, including the ICO, the government has decided to implement a 29.8% increase in data protection fees across all tiers, slightly below the initially proposed 37.2%. The existing three-tier structure for fee determination will be retained, as will the £5 discount for Direct Debit payments and the current exemptions from the requirement to pay a fee. The government acknowledged concerns from some respondents about the impact of fee increases on micro and small businesses and public sector bodies, especially in the current economic climate. There were also calls for greater transparency regarding how the increased fees would enhance the ICO's services and provide value for money to fee-paying organisations. The government has shared this feedback with the ICO to address areas where service improvements are desired. These adjustments aim to balance the need for the ICO to be sufficiently resourced to uphold data protection laws while considering the financial pressures faced by smaller organisations.	**Action Required:** • Read the full publication here.

Update	Summary	Action for firms
Legal Dispute – Jurisdictional clauses Applies to: International firms	In the intricate landscape of reinsurance agreements, the recent cases involving Tyson International Company Limited (Tyson) underscore the critical importance of clarity in contract documentation, especially concerning dispute resolution provisions. These cases highlight the potential for costly jurisdictional disputes when multiple agreements with conflicting terms are executed. **Case Summaries:** **Tyson v. Partner Reinsurance Europe SE**: In this instance, Tyson and Partner Re initially executed a reinsurance contract using the Market Reform Contract (MRC), which stipulated English law and exclusive jurisdiction of English courts. Subsequently, they issued a Market Uniform Reinsurance Agreement (MURA) covering the same subject matter but specifying New York law and arbitration. The Court of Appeal determined that the MURA superseded the MRC, thereby enforcing the New York arbitration clause. **Tyson v. GIC Re, India, Corporate Member Ltd**: Tyson and GIC Re entered into an MRC followed by a MURA. However, the MURA, in this case, included a 'Confusion Clause' stating that the MRC would take precedence in case of any conflict. The Commercial Court upheld that the English jurisdiction clause in the MRC prevailed over the New York arbitration clause in the MURA, granting an anti-suit injunction to restrain the New York arbitration. These cases serve as a cautionary tale, emphasizing the necessity for meticulous attention to detail in contract formulation within the financial and insurance sectors. By proactively addressing these considerations, firms can mitigate the risk of jurisdictional conflicts and ensure that dispute resolution mechanisms align with their strategic objectives.	**Key Takeaways for Financial Firms:** **Consistency in Contractual Documents**: Ensure that all contractual documents related to the same transaction are consistent, particularly concerning dispute resolution clauses. Inconsistencies can lead to protracted legal battles over jurisdiction and applicable law. **Hierarchy and Precedence Clauses**: Incorporate clear hierarchy or precedence clauses to specify which document governs in the event of a conflict. This can prevent ambiguity and provide clarity in dispute resolution scenarios. **Comprehensive Review Process**: Implement a thorough review process when issuing and executing standard market contracts. Even widely accepted forms like the MRC and MURA should be carefully examined to ensure alignment with the parties' intentions. **Awareness of Jurisdictional Implications**: Be cognizant of the jurisdictional implications of the chosen dispute resolution mechanisms. The selection between arbitration and court proceedings, and the choice of law, can significantly impact the strategy and outcome of potential disputes.

Update	Summary	Action for firms
Proposed ban on ransomware payments Applies to: All firms	On January 14, 2025, the UK government initiated a public consultation to address the escalating threat of ransomware attacks. Ransomware is malicious software that compromises a victim's computer system, often leading to data theft and operational disruptions, with attackers demanding payment for restoration. **Targeted Ban on Ransomware Payments for Public Sector and Critical National Infrastructure (CNI):** This proposal suggests prohibiting public sector entities, including local authorities and operators of CNI, such as the NHS, schools, and transportation networks, from making ransomware payments. The consultation also seeks feedback on whether essential suppliers to these sectors should be included and the appropriate penalties for non-compliance, which could range from civil fines to criminal charges. **Ransomware Payment Prevention Regime:** Under this regime, organisations and individuals not covered by the targeted ban would be required to report any intention to pay a ransom to authorities before proceeding. The authorities would then assess the situation and provide guidance, potentially blocking payments if they violate legal constraints, such as sanctions. **Mandatory Ransomware Incident Reporting:** This proposal mandates that all ransomware incidents be reported to authorities, regardless of whether a ransom payment is intended	**Actions to take:** • To read and engage with the consultation, please visit this page.

RR COMPLIANCE associates

RR Compliance Associates are a trading style of R&R Compliance Consultants Ltd, a limited company registered in England and Wales (company number 12070286). Our registered office is 51 Lime Street, London, EC3M 7DQ. VAT number 326 1938 96.