Tuesday, 08 April 2025

Dear Charlie,

We write to you collectively on behalf of the financial services industry regarding the Home Office's legislative proposals on ransomware. The industry is committed to combating economic crime, and we support the government's efforts to disincentivise cybercrime and improve cross-sector resilience, safeguarding consumers, and upholding trust in the digital ecosystem. However, while we understand the Home Office's intention, we are concerned that the proposals raise major operational challenges, may fail to address the government's objectives, and, in some cases, appear unfeasible.

The outright ban on ransomware payments by private sector UK critical national infrastructure (CNI) and the proposed payment authorisation regime could both have unintended and potentially severe consequences and may not be effective in reducing the threat that ransomware poses to the UK. More detail is needed on the scope of the proposals, particularly the extent to which the CNI classification and, therefore, the application of the payment ban, applies across financial services. The Home Office must also clarify how liability would be applied in practice, and we recommend a further consultation period with the private sector. At a minimum, the ban and payment prevention scheme should retain a level of flexibility if a disruption would potentially cause significant consumer impact, threaten the safety and soundness of the firm, or pose a financial stability risk to the UK economy.

The incident reporting proposals also require further streamlining and harmonisation with existing requirements and should support intelligence sharing through current information sharing groups. We are concerned that the proposals fail to consider and leverage the significant work underway to bolster resilience and address cybercrime across the financial services industry. Several regulatory and voluntary initiatives have successfully grown and matured in recent years, for example the Cyber Defence Alliance (CDA), the Financial Sector Cyber Collaboration Centre (FSCCC) and our sector regulators' own incident reporting requirements. Many of these groups also have a government presence.

As an overarching comment, implementing a stricter approach than other major financial jurisdictions could create costs and risks putting UK firms at a potential disadvantage. This could harm the UK's competitiveness as an international financial centre and stifle wider economic growth.

Proposal one: Ransomware payment ban for CNI

The financial services industry understands the implications of paying criminal enterprises and supports the intention to disincentivise ransomware attacks across CNI by removing the possibility of receiving payment. However, our concerns are as follows:

- Paying a ransomware request can be essential to avoid large-scale operational disruptions. Given the financial services industry's systemic importance to businesses, public sector institutions, consumers and the overall UK and global economy, the impact of such disruptions could be widespread and severe. This could range from leaving consumers unable to pay their rent or buy food or, given the global interconnectivity of financial markets, triggering a ripple effect across supply chains that causes widespread economic instability, liquidity crises, and a

loss of confidence in UK financial services. The ban may also 'paralyse' the insurance sector due to uncertainty over whether they can support firms who have experienced an attack.

- Financial services are uniquely placed as the industry that is likely to process payments relating to ransomware. A financial institution should not be liable for processing ransomware payments instructed by the customer, even if there is reason to believe or suspect that it is a ransomware payment. Financial institutions are often unaware of the purpose of the payment and have a regulatory requirement to process payments if requested by the customer, irrespective of concerns relating to fraud. Intermediaries regularly advise impacted firms not to inform their financial institutions if they are facing a ransomware attack.
- Making a ransomware payment a civil or criminal offence would effectively create a double victimisation scenario. To mitigate the legal risk associated with a criminal conviction, financial services would likely have to significantly increase due diligence in relation to the processing of payments, creating a less efficient business environment in the UK. As noted elsewhere, the focus should be on strengthening firms' operational resilience.
- International precedents suggest that a payment ban would more likely drive payments underground or redirect attacks than deter criminals. This could disproportionately impact small and medium-sized enterprises (SMEs), who may have less mature cybersecurity capabilities.

While we do not support a ban on ransomware payments by the financial services industry, if the Home Office proceeds it must clarify:

- The scope of CNI across financial services, including whether it would include critical third parties for the financial sector. The Financial Conduct Authority (FCA) currently regulates over 40,000 firms across the UK financial services industry, with great variety in size and systemic importance. Applying the ban across all these firms would be disproportionate and would not reflect a targeted approach.
- Liability regarding the ransomware payments. It is not clear whether the payment processor (who may not know the intended purpose of the payment) would also have liability, and how the government would enforce this in practice should the ban be determined a criminal offence. Due to the lack of information provided in the initial consultation, a further consultation phase is needed where the industry can comment on how liability would be apportioned in practice.

Proposal two: Ransomware payment prevention regime

We welcome the intention to help firms that are victims of a ransomware attack and improve understanding of the cybercrime landscape. However, introducing delays in cyberattack responses will exacerbate business, legal, and reputational risks during a period of severe disruption. In particular:

- These proposals would require firms to seek government approval at a critical moment when they could be facing significant disruption in their operations, with severe reputational risks or even bankruptcy. Any delays during this period could force more extreme disruptions at significant cost to businesses and consumers. This could put firms in the position of deciding between no notification and committing a criminal offence, or bankruptcy. The government could itself face litigation and damages claims if stopping payments could cause a company to face insolvency.

- Greater clarity is needed on how the Home Office would resource these proposals, which would require significant and expert government support to be available 24 hours a day and 7 days a week, and to make high-impact decisions in a rapid timeframe with limited information.
- It is not clear from the proposals what rationale would inform decisions to block a payment. The government should proactively share any relevant intelligence with financial institutions, helping firms to make informed decisions.

Proposal three: Ransomware incident reporting regime

We recognise the potential advantages of a mandatory ransomware incident reporting regime and welcome the government's intention to align this with parallel initiatives, such as the upcoming Cyber Security and Resilience Bill. However:

- The UK financial services industry is already heavily regulated, and firms are required to report "material" events to regulators. Broadening this out would have a significant operational impact on firms. Any financial sector reporting should be aligned with existing reporting requirements (for example, FCA CP24/28 and Prudential Regulation Authority CP17/24) and be reported to these regulators. While strong regulation and oversight can support safety and stability across the financial services industry, a harmonised and centralised approach is essential to avoid a disproportionate burden on firms, ultimately stifling the industry's role as an enabler of economic growth.
- The financial services industry already participates in existing information-sharing groups with government presence, such as the National Cyber Security Centre (NSCS) and National Crime Agency (NCA). The government should leverage these for periodic updates on near-misses or low-impact events rather than formalising incident reporting within the first 72 hours, which could divert resources from ongoing incident management activities.

Next steps

Overall, while we support the Home Office's efforts to combat ransomware and enhance the resilience of the UK's digital ecosystem, the proposals require significant refinement. It is essential to consider the financial services industry's systemic importance and the potential ripple effects of any disruptions. We urge further consultation with the industry to clarify the scope and enforcement of these measures. The government could consider a phased approach commencing with voluntary reporting before assessing whether additional mandatory requirements are beneficial. The top priority should be prevention through ongoing industry resilience efforts rather than reporting or deterring payments.

To ensure a joined-up government cyber security strategy, the Home Office must coordinate closely on these proposals with the Cabinet Office, the Department for Science, Innovation and Technology, HM Treasury, government cyber security entities and financial regulators. A joined-up approach is key to effectively combating ransomware without disrupting critical operations.

Kind regards,

TheCityUK, The Investment Association (IA), The Association for Financial Markets in Europe (AFME), The Futures Industry Association (FIA) and The Personal Investment Management & Financial Advice Association (PIMFA).