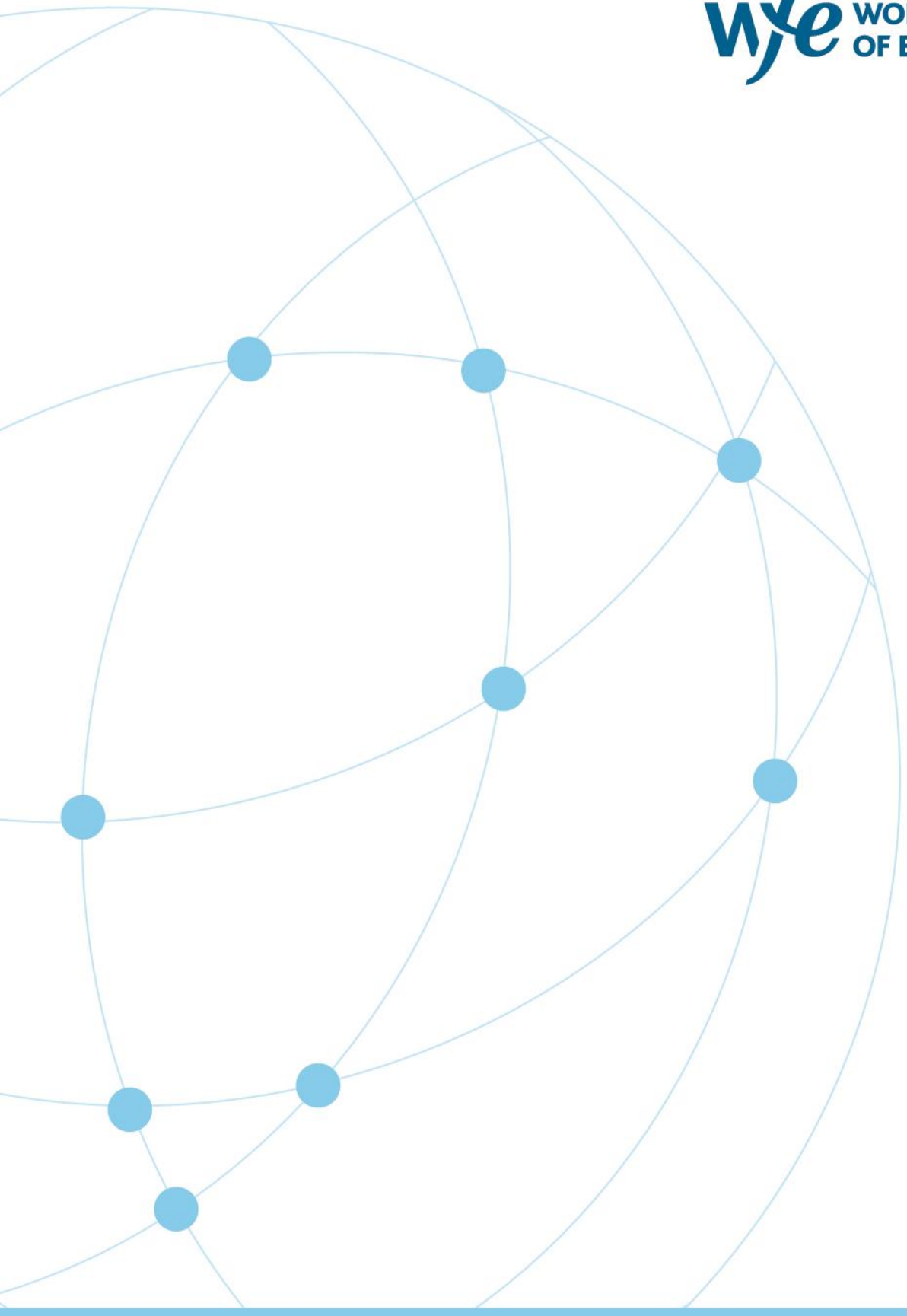

WFE response on Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting

7th April 2025

Background

Established in 1961, the World Federation of Exchanges (WFE) is the global industry association for exchanges and central counterparties (CCPs). Headquartered in London, it represents over 250 market infrastructure providers, including standalone CCPs that are not part of exchange groups. Of our members, 37% are in Asia-Pacific, 43% in EMEA, and 20% in the Americas.

The WFE's 87 member CCPs and clearing services collectively ensure that risk takers post some $1.1 trillion (equivalent) of resources to back their positions, in the form of initial margin and default fund requirements. WFE exchanges, together with other exchanges feeding into our database, are home to over 49,000 listed companies, and the market capitalisation of these entities is over $116.58 trillion; around $155 trillion (EOB) in trading annually passes through WFE members (at end 2024).

The WFE is the definitive source for exchange-traded statistics and publishes over 350 market data indicators. Its free statistics database stretches back 49 years and provides information and insight into developments on global exchanges. The WFE works with standard-setters, policy makers, regulators, and government organisations around the world to support and promote the development of fair, transparent, stable and efficient markets. The WFE shares regulatory authorities' goals of ensuring the safety and soundness of the global financial system.

With extensive experience of developing and enforcing high standards of conduct, the WFE and its members support an orderly, secure, fair, and transparent environment for investors; for companies that raise capital; and for all who deal with financial risk. We seek outcomes that maximise the common good, consumer confidence and economic growth. And we engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in a globally integrated financial system.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

Chhavi Sinha, Manager, Regulatory Affairs: csinha@world-exchanges.org
Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org
Nandini Sukumar, Chief Executive Officer: nsukumar@world-exchanges.org

Response

The UK Home office recently launched a public consultation on legislative proposals aimed at combating ransomware threats in the UK. The three key proposals include:

1. **Banning ransomware payments** by public sector bodies and owners and operators of Critical National Infrastructure ("**CNI**"), such as energy supply, water supply, transportation, health, and telecoms;
2. **Introducing a ransomware payment prevention regime**, requiring victims to engage with authorities before making payments, with the potential for payments to be blocked.
3. **Implementing a ransomware incident reporting regime**, mandating the reporting of ransomware attacks and related payments.

While the proposals primarily target the public sector and CNIs, there is a possibility that UK market infrastructures (FMIs, ie exchanges, clearing houses and central securities depositories) could also be impacted, as some entities fall within the CNI classification under the National Protective Security Authority.

As a global industry association representing exchanges and central counterparties (CCPs), the World Federation of Exchanges (WFE) supports the UK Government's objective of reducing ransomware payments to deter cybercriminals and enhance law enforcement's ability to disrupt and investigate ransomware activities. However, we have significant concerns regarding the practical implementation of **Proposals 1 and 2**.

Many UK financial services firms and FMIs provide critical financial functions that require swift recovery from ransomware incidents. In some cases, organisations may need to make a payment to ensure business continuity / respect recovery time objectives or to minimize reputational, data, and operational impacts. Penalizing such decisions with criminal or civil sanctions could impose undue operational and financial burdens **(Proposal 1).** Furthermore, if only one jurisdiction bans ransomware payments while others do not, it may fail to effectively disrupt the ransomware business model, as intended by the proposals.

The proposed **ransomware payment prevention regime (Proposal 2)**, which mandates engagement with authorities before making a payment and grants them the power to block payments, could lead to delays in urgent situations requiring round-the-clock expert assessment. Such delays could increase financial and systemic risks, particularly for institutions that rely on real-time operations. UK authorities may need to expand availability and expertise in order to provide this service and will have to consider how to support real-time operations.

Moreover, the financial services are different from the other public sectors and CNIs (listed in the proposal) as they are most advanced and already subject to most intense oversight/stringent regulation. Due to their distinct nature and expertise, the financial services sector should be exempt from the current proposal, given the maturity of cyber, risk, and resilience programs and existing oversight. If the same regime is to be applied, financial services firms should be given the flexibility to determine whether and when to make ransomware payments. To strike the right balance between effectiveness and proportionality, we urge the UK Government to **prioritise resilience-building measures**—such as improved cybersecurity, robust backup systems, and enhanced computer security—rather than rigid payment restrictions. We also recommend stronger **regulatory oversight and stricter controls over the use of cryptocurrency transactions**, given their frequent use in ransomware payments.

Additionally, we have concerns about **Proposal 3 (ransomware incident reporting regime)**, particularly the duplicative nature of reporting requirements. UK financial institutions already report cybersecurity incidents to regulatory bodies, and the proposed regime does not clearly define the scope of reportable incidents. Key questions remain, such as

whether incidents occurring overseas would need to be reported and how such requirements would align with international regulations. We encourage relying on existing regulations and requirements for incident reporting.

Finally, we encourage a measured approach that balances deterrence with practicality, ensuring that regulations support, rather than hinder, the resilience of UK financial markets. Financial services firms should be exempt based on existing regulations and oversight and should continue to make decisions based on their risk appetite and potential business impact.

We appreciate the opportunity to contribute to this consultation and look forward to further engagement on this important issue.