Consultation Response

Ransomware: Home Office proposals to increase incident reporting and reduce payments to criminals

April 2025

AFME welcomes the opportunity to respond to the Home Office proposals to increase incident reporting and reduce payments to criminals.

AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors, and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

We are responding from the perspective of our bank members on the assumption that all regulated financial entities will be within scope as Critical National Infrastructure (CNI). There has been a high level of interest in this consultation given the potential for unintended consequences, but we welcome the Home Office's ambition to reduce ransomware payments to cyber criminals and to secure enhanced visibility over ransomware threats targeting UK businesses. Ransomware represents a material cyber security threat that should be counteracted by government support. The financial sector stands ready to cooperate with the government to make the UK a hostile environment for malicious threat actors.

However, the sector is concerned that the three proposals in the ransomware proposal could incur significant unintended negative consequences, and would encourage a full cost:benefit analysis to ensure these consequences are identified in advance of the proposals proceeding to implementation. The financial sector encourages that all elements are considered and a further Consultation Paper, with greater detail and clarity, is put forward by the Home Office. Our primary concerns are:

1) The targeted ban on ransomware payments, without any flexibility, is difficult to operationalise, poses risks to financial stability and raises the cost of doing business in the UK.
2) The Home Office intervention in a ransomware incident could complicate responding to an incident during a period that could result in bankruptcy.
3) Incident reporting for ransomware to aid law enforcement is logical but should remain targeted and predicated on actionable information for authorities.

The financial sector therefore encourages the Home Office to add more flexibility to their proposals and to consider a Government-wide approach to improve the cyber defences of all organisations operating in the UK. The planned Cyber Security and Resilience Bill represents a positive development that will create a more difficult environment for malicious actors to operate in the UK.

In the three sections below, we elaborate on each of our concerns. We would welcome an opportunity to discuss our concerns further, and to highlight how ongoing work by the Bank of England (BoE) and Financial Conduct Authority (FCA) could be better leveraged as part of the Home Office's fight against ransomware. We would also encourage the Home Office to clarify

the scope of the incoming requirements, for example in relation to firms headquartered outside the UK or who explicitly is regarded as CNI.

We remain available to discuss any of the specific points in further detail. Please do not hesitate to contact the team via marcus.corry@afme.eu.

Proposal 1: Targeted Ban on Ransomware payments

The introduction of a total ban on ransomware payments - even on a targeted basis - is a blunt tool which will likely have unintended consequences that are not adequately considered in the Options Assessment. As a result, we are concerned that the ban cannot be effectively operationalised and will have a significant adverse impact on the financial sector. Furthermore, we request clarifications on key elements of the proposal. We elaborate on each of these issues directly below.

Inability to operationalise the ban

The nature of ransomware attacks, and the malicious actors who utilise them, complicates operationalising the ban. Specific issues that were not considered in the proposal include:

- **The global nature of cybercrime undermines effectiveness.** Malicious actors target companies and individuals globally. Therefore, implementing a ban in a single jurisdiction is unlikely to disrupt their business model and causes complications for businesses with global coverage (for example, an organisation based in multiple countries; a UK business using a system which also supports other non-UK businesses; and a system supporting a UK business which is located and administered outside of the UK). The financial sector supports global standards where possible and believes any proposals should consider existing efforts in other jurisdictions who are members of the Counter Ransomware Initiative.
- **Monitoring ransom payments is complex, and further consultation is required to determine who is liable for payments.** Ransomware payments are often processed by intermediaries who operate across jurisdictions and pay via non-traditional financial institutions. Furthermore, intermediaries often encourage impacted firms to not inform financial institutions that a ransomware attack is occurring. As a result, payments often occur without the financial institutions being informed that the payment is for a ransom. This is especially the case where there are multiple parties involved in a transaction or with regards to transparency over Nth party providers. The Home Office's proposal introduces legal uncertainty regarding what body is liable for the ransomware payment and should provide further clarity regarding their intent, or not, to ban the processing of payments. The sector would have to enforce stricter payment processing due diligence across all payments to comply effectively with the ban. This could impact legitimate payments, which are mistaken for ransomware payments due to the need make near real-time decisions, and drive up the cost of doing business in the UK. Liability could also apply to multiple individuals within the impacted firm, the intermediary, or the firm processing the payment. A further consultation is required with detail regarding liability before any proposal should be enacted by the Home Office. Currently the proposed mix of criminal and civil penalties causes concern without providing any detail on the mechanisms for enforcement.

- **The UK government may wish to consider other proposals for small businesses given the opportunistic nature of ransomware threats and the impact they could have on small businesses.** Financial institutions threat intelligence shows that malicious actors target small businesses because they have lower cyber defences and do not face the reputational risk to pay the ransomware payment. Malicious actors additionally may perceive that law enforcement are less interested in ransomware attacks on smaller businesses in comparison to CNI. Small business might not be able to return to business as usual without paying a ransom. As a result, they might face market disruptions and, in a worst-case scenario, even bankruptcy. The financial sector believes this would significantly increase the risk of doing business in the UK.

Adverse impact on financial sector

Financial institutions are disproportionately impacted by a blanket ban on ransomware, both in terms of the impact on their consumers to and the uncertainty regarding liability.

- **All of the financial sector is regulated and therefore the sector-ban for regulated entities applies broadly.** The Financial Conduct Authority (FCA) regulates approximately 41,500 organisations that represent a range from globally systemic firms that operate across numerous jurisdictions to small retail and consumer-focused financial firms with limited operations and cybersecurity capabilities. A unilateral ransomware payment ban would disproportionably apply to the financial sector due to the number and range of organisations in-scope. The scale of the impact within financial services also fails to sync with the Home Office's view that only 1% of private sector participants would be caught by the proposed ban.
- **A ransomware attack on a financial institution could negatively impact consumers and potentially cause systemic market-wide disruptions.** The ransomware ban would apply to all financial institutions. This is a sector with strong cyber defences and business continuity capabilities. In extreme circumstances, a payment could be quickest means for a financial institution to mitigate the loss of availability for financial services. A disruption could result in the loss of banking access or use of financial services to consumers across the UK. Other systemic firms operating in wholesale markets across jurisdictions could face disruptions that have market-wide or global impacts. Any ban introduced by the Home Office should allow flexibility in extreme scenarios where there is substantial risk to consumer access to financial services or there could be market-wide impacts to the UK economy.
- **Engagement is required with the Treasury, Bank of England, and the Sector Response Framework in order to consider the sectoral impact of such restrictions.** Particular thought needs to be given to how this ties into wider resiliency discussions, for example the length of time a firm can withstand a ransomware attack, the dependencies/ interconnected services, and knock-on repercussions. Further thought should be given to second order effects such as to the cyber insurance market and associated increases in costs there.

Proposal 2: A new ransomware payment prevention regime

An enforced payments-prevention scheme would place a UK Government authority in the middle of a ransomware incident where the organization could be facing a severe outage of their services. Any guidance or approval scheme would require immediate responses by the authority

or intermediaries and impacted organizations will struggle to adhere to the scheme. Firms would call on the Home Office to ensure sufficient resourcing is secured and in place before proceeding with this approach. There is a vast responsibility on designated CNI's and government entities to ensure their controls are provably embedded, robust and assured enough to tackle ransomware. It is likely the Government's proposed role will be subject to considerable scrutiny following an incident, and could result in litigation.

It also remains unclear how this regime would work in practice, for example if the Home Office intends to provide tags or markers to support with the identification of such payments, especially where the bank does not have visibility of indicators of compromise, and if this relates to all forms of payment including for instance, via cryptocurrency. A set of thresholds are widely envisaged in terms of the scope of the regime, and we suggest these are based on organization size, ransom amount, potential contagion risk etc. Greater clarity is also needed over the extent and format of information which affected firms are expected to provide, and what support they can expect. The Home Office should additionally incorporate any insights from other Government agencies into the decision making process.

Finally parity is needed across regulators in key jurisdictions, in particular the US and UK to ease the administrative burden for firms. The Home Office should be speaking with regulators in other jurisdictions to avoid significant divergence in requirements or approach to reporting, leveraging existing venues including the G7 Cyber Experts Group, IOSCO and other public-private partnerships. Firms should not be subject to legal repercussions for struggling to adhere to divergent regimes simultaneously.

Proposal 3: A ransomware incident reporting regime

The financial sector recognises that a ransomware incident reporting regime that provides law enforcement with actionable information concerning malicious actors would aid the authorities' capabilities to create a hostile environment. Nonetheless, the sector would encourage further clarity regarding the scope of ransomware incidents and a focus on realised ransomware incidents instead of suspected.

- **A focus on 'suspected' ransomware incidents could result in overreporting.** Suspected ransomware incidents could result in a large scope of incidents for financial institutions, notably if any data extortion incident is considered in-scope. Incident reporting should be focused on actionable information and realised incidents to reduce the scope and create a more proportionate regime. There are numerous other avenues and forums by which authorities can gather data on ransomware's threat profile. Those which the financial sector participate in include the NCA, the NCSC and the BoE's Sector Response Framework.
- **Actionable information should directly aid law enforcement capabilities.** The incident regime should be subject to a further consultation where law enforcement clearly defines what information is actionable subject to clear definitions and thresholds in aiding their ability to counter malicious actors. There is a risk that a regime could result in high reporting but, due to a lack of actionable or tangible information, results in minimal aid to authorities. At worst, it may detract resources from incident management, unintentionally exacerbating the risk. A voluntary scheme focused on material information could be of greater aid to authorities. A regime for information awareness regarding payment figures, in contrast, should not require high levels of information from impacted firms.

- **The financial sector is subject to existing incident reporting regimes.** The Home Office should be mindful of similar supervisory initiatives being undertaken in other sectors or in other jurisdictions. The financial sector is currently being consulted on an incident reporting regime by the FCA and the Bank of England. In this respect, the financial sector supports the Home Office in engaging with financial regulators and supports reporting to a single portal or institution, through a harmonised and centralised approach.

AFME Contacts

Marcus Corry
marcus.corry@afme.eu
+44 (0)20 3828 2679

Coen Ter Wal
coen.terwal@afme.eu
+44(0) 20 3828 2727