COMBATING RANSOMWARE

Would Recent Developments Change Business Decision-making?

| By ADV. VERED ZLAIKHA

Adv. **VERED ZLAIKHA**
Partner at Lipa Meir & Co. Advocates and Head of Cyber Affairs & AI Practice

Ransomware is a form of malware that blocks access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring the victims' access to their systems or data.

On October 13, 2020, the G7 expressed concern about ransomware cyber-attacks and adopted a "Ransomware Annex to G7 Statement". According to the Annex, ransomware attacks against critical infrastructures such as hospitals and financial institutions in G7 countries have been increasing in scale, sophistication, and frequency, while illicit actors have exploited COVID-19 to conduct the attacks**. The Annex mentions the significant economic damage caused by ransomware**, as well as threats to customer protection and data privacy. It recognizes the **broad spectrum of malicious actors and motives** behind ransomware, such as criminal activities, transnational organized crime, terrorism, and state-sponsored acts to finance the proliferation of weapons of mass destruction. The frequent demand of ransoms for virtual assets is of particular concern.

In accordance with the Annex, the G7 is committed to working with financial sectors in those countries to combat ransomware. The Annex emphasizes the following:

• The G7 commits to **coordinated action** to mitigate this threat. Coordinated responses will encompass where possible information sharing (including financial intelligence and cyber techniques); economic measures (including the option of targeted financial sanctions against ransomware operators and their facilitators); support for effective implementation of the FATF [Financial Action Task Force] standards; and the promotion of available technical innovations to protect cyber assets.

(Freepik.com)

• As the payment of ransom entails financial activity, it is **subject to anti-money laundering and counter-terrorist financing laws and regulations**. Financial institutions and the public are called upon to be especially alert to prevent sanction evasion in line with their national legal obligations.

• Aside from financial institutions, **even companies whose primary business is not financial services, such as cyber-incident consulting firms**, may fall under the obligations for financial institutions if they provide qualifying services, such as money transfers.

• The G7 notes the importance of virtual asset service providers having **effective programs in line with the FATF standards and national obligations**. It calls upon companies to move "beyond traditional perimeter security to defend against ransomware." Companies are also advised to consider **altering their own internal response and recovery plans** in light of the potential sanction violations, particularly if current plans consider paying a ransom.

Shortly before the G7 announcement, similar steps were addressed by the US Treasury Department. **On October 1, 2020, the US Department of the Treasury issued two advisories to alert companies about ransomware risks**. The Treasury's Financial Crimes Enforcement Network (FinCEN) issued *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*. It refers, inter alia, to the involvement of digital forensic and incident response companies, cyber insurance companies, and money service businesses in facilitating ransomware payments to cyber criminals. It highlights their legal obligations in relation to money laundering under US laws and regulations. The Office of Foreign Assets Control (OFAC) issued *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, which highlights the sanction risks associated with facilitating ransomware payments on behalf of victims, and encourages financial institutions and other companies (such as those involved in providing cyber insurance, digital forensics, and incident response) to implement a risk-based compliance program to mitigate exposure to sanction-related violations.

As it was discussed in the media, the steps taken in the US were accepted with criticism and mixed reactions. Some suggested that insurance companies have already taken the relevant legal duties into account, thus one should not expect a significant change following those advisories. Others posited that insurance companies might reconsider ransomware insurance coverage. It was also argued that these steps would complicate an already challenging decision, especially in regards to SMEs, and that it might cause victims to hesitate more before they involved law enforcement authorities.

To sum up, the Ransomware Annex seems to reflect a political desire for a joint effort to combat the growing cyber threat to businesses, especially during COVID-19, by sharing information and implementing accepted standards in the areas of anti-money laundering and counter-terrorist financing**.** Such global cooperation may be easily developed, as it is based on existing legal frameworks in these areas, including national legislation. **It remains to be seen how this step would be implemented and what its effects would be**, especially in light of the mixed reactions in the case of the US advisories**.** Apparently, even in the absence of a conclusive rule excluding ransom payment, **strengthening adherence to anti-money laundering and counter-terrorist financing rules in the context of ransomware may gradually influence** G7 markets and possibly affect norms of behavior in other markets as well with respect to the **calculus in ransom payment of victims and their service suppliers**. The latter group, which includes incident response and forensics companies, as well as insurance companies, may update risk assessments and their risk-based compliance programs,in order to minimize exposure to regulatory violations. Companies that these developments may be relevant to their activities, should follow these developments, and consider their specific circumstances with their legal advisers.

The writer is a Partner at Lipa Meir & Co. Advocates and Head of Cyber Affairs & AI Practice.

WINTER 2020
THE JERUSALEM POST
Commercial department

· LEGAL · EDITION