Article Information

Authors: Michael Bacina, Steven Pettigrove, Jake Huang
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

To pay or not to pay? Ransomware and sanctions risk

Michael Bacina, Steven Pettigrove and Jake Huang of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

Ransomware attacks – victims of which are extorted to pay a ransom – have become increasingly prevalent and sophisticated in recent years. When a ransomware victim is confronted with the hard question of "to pay or not to pay" hackers, there are a number of legal, ethical and practical matters to consider, and the risks of breaching sanctions laws may not immediately be front in mind. In this article, we will discuss the nature of ransomware and the easily overlooked sanctions risks associated with ransomware payments.

Sanctions risk is of course just one risk to consider when dealing with a ransomware scenario and we recommend seeking professional advice from cybersecurity specialists, intelligence firms and lawyers who have experience in relation to cyber and ransomware attacks if you are dealing with a ransomware incident.

The threat of ransomware

The *2023–2030 Australian Cyber Security Strategy* (**Strategy Report**) published by the Australian government calls ransomware

> one of the most disruptive cyber threats in the world today.

Companies of different sizes and industries, spanning from multinational law firms to financial institutions, energy companies and even governments have become targets of high-profile ransomware attacks, due to the valuable data and sensitive information they hold.

The Australian government said they are working hard to crack down on ransomware attacks, but this is no easy task. As the Strategy Report admits, with new technologies like automated ransomware attack software being developed, and "ransomware-as-a-service" products ready for purchase on the dark web, it is becoming easier than ever for criminals to steal valuable data.

So what if your business unfortunately falls victim of a ransomware attack? When "to pay or not to pay" becomes a very real question, would you choose to comply?

Facing such tough questions, individuals and businesses might quickly put their mind to practical issues such as where they can source the ransom (often demanded in cryptocurrencies nowadays) or whether their insurance policy will cover such payment. However, it is easy to neglect the risk of breaching applicable sanctions laws by making a ransomware payment.

Does the law expressly prohibit making ransomware payments?

There is no law in Australia that expressly, or blanketly prohibits a person or entity from paying ransom to a cyberattacker. The government's attitude, as evidenced in the Strategy Report, seems to be discouraging but not forbidding ransomware payments:

> The ransomware business model is fuelled by payments made to cybercriminals, with cryptocurrency transactions enabling malicious actors to anonymously profit from extortion claims. Paying a ransom does not guarantee that sensitive data will be recovered. It also makes Australia a more attractive target for criminal groups.

However, it is possible that making a ransomware payment could breach sanctions laws in both Australia and other jurisdictions where the ransomware hacker is subject to government sanctions.

Sanctions risks

Most jurisdictions including Australia and the United States apply targeted sanctions to persons listed on applicable sanctions lists as well as comprehensive, sectoral or product specific sanctions programs which apply to specific jurisdictions or certain goods and commercial activities (we refer below to these persons as **Sanctioned Persons**). Making a payment to a Sanctioned Person, be it a ransomware payment or not, may trigger a breach of sanctions laws.

Many notorious ransomware hackers have been expressly designated to be Sanctioned Persons (i.e. by being placed on a sanction list) by governments. Others that are not designated may well be sanctioned for other reasons, such as operating from a comprehensively sanctioned jurisdiction.

In both Australia and the US, breaching sanctions laws may result in serious consequences, including exposing entities and/or their employees to criminal and civil liabilities. Sanctions liability can be imposed even where an entity or individual is not aware that it was dealing with a sanctioned party (so-called “strict liability”).

Individuals or entities based in Australia will certainly be subject to Australian sanctions laws, but they must also pay attention to US sanctions laws. This is because the US adopts a broad view of its jurisdiction in applying and enforcing US sanctions laws and regulations. This means that foreign persons may also become subject to US jurisdiction depending on whether a jurisdictional nexus is established and, under certain sanctions regulations, the US may apply so-called “secondary sanctions” to foreign persons, that is the risk of being added to a list of sanctions targets, for engaging in certain dealings with US sanctions targets.

Furthermore, sanctions laws from different jurisdictions may apply separately or concurrently depending on whether an activity or person has a nexus with the jurisdiction for sanctions purposes. This may include other jurisdictions such as the UK and European Union. Even where a person or entity may fall outside the jurisdiction of applicable sanctions laws, legal and reputational consequences may still apply to dealing with Sanctioned Persons.

What should you do to avoid breaching sanctions laws?

The first step is to identify the name, jurisdiction of, or type of activity engaged in, by the ransomware hacker and whether the hacker is listed on any sanctions lists. While this is may not always be sufficient to address the risk of dealing with Sanctioned Persons, thorough investigations must be done before making any payment. A good record of such investigations will be vital to prove that you have exercised your due diligence.

You will also need the help of professional cybersecurity specialists, intelligence firms and lawyers who have experience in relation to cyber and ransomware attacks. They can advise and guide you through every step, and minimise your risks as much as possible. Sanctions risk is just one factor to consider and there will be other ethical, practical and legal factors to assess such as the risk that the hackers will not make good on promises to release data or that the payment may further feed ransomware attacks.

It is also worth noting that when it comes to cryptocurrency ransomware payments, blockchain investigations and the screening of wallet address on sanctions lists are some of the key steps you must take. That’s why specific expertise in these areas is what you should be looking for.

Conclusion

No one wants to deal with ransom hackers and cyberattackers, and paying them is certainly not encouraged. However, when the question of “to pay or not to pay” becomes a real risk for your business, you must contemplate all factors which may influence this decision, including sanctions risks. The golden rule is always to reach out for professional help when you are not sure what to do.