ACAMS

SANCTIONS SPACE

SANCTIONS MASTERCLASS SERIES FOLLOW-UP BRIEFING PAPER

NEXUS OF CYBER, RANSOMWARE AND SANCTIONS COMPLIANCE

Background

This paper builds upon information provided in the ACAMS Sanctions Masterclass: Nexus of Cyber, Ransomware and Sanctions Compliance. Together with the ACAMS team, this session was developed in conjunction with Jamie Boucher, Skadden, Arps, Slate, Meagher & Flom LLP, and Andrew Jensen, Scotiabank, with wider contributions from Chris Po-Ba, Lloyd's of London. This briefing should be read alongside **viewing the Masterclass** and downloading the accompanying slides.

What is Ransomware and How Significant is the Threat?

Ransomware is generally considered to be a form of malicious software, also known as malware, which is usually designed to prevent access to a computer system and/or data, potentially by encrypting data or programs. This is done in order to extort ransom payments from victims in exchange for decrypting the information and restoring access to the blocked systems or data. Payments are usually demanded through digital currency, such as Bitcoin.

In recent years, there has been a substantial rise in both the scale and scope of ransomware attacks.[1] In parallel, the volume and quantity of payments are also escalating – for example, roughly $350 million in ransom was paid to malicious cyber actors in 2020, an increase of over 300% on the previous year.[2] As a result of these trends, ransomware has been of significant and increasing focus for governments around the world, as demonstrated by the commitment to fight ransomware made at the 2021 G7 Summit.[3] Against this background, ransomware is now recognised as one of the most immediate and highest impact cyber threats identified by a number of jurisdictions, such as the US, UK, Canada, and Australia.[4]

[1] ENISA Threat Landscape 2020 - Ransomware (europa.eu)
[2] United States Government Launches First One-Stop Ransomware Resource at StopRansomware.gov | Homeland Security (dhs.gov)
[3] FACT SHEET: G7 to Announce Joint Actions on Forced Labor in Global Supply Chains, Anticorruption, and Ransomware (whitehouse.gov)
[4] Mitigating malware and ransomware attacks (ncsc.gov.uk); Canadian Centre for Cyber Security: National Cyber Threat Assessment 2020 (cyber.gc.ca); Locked Out: Tackling Australia's ransomware threat (homeaffairs.gov.au)

Masterclass Overview

The Masterclass addressed the challenge of ransomware attacks and payments, specifically within the context of sanctions compliance. The agenda included:

- a brief geopolitical overview covering key definitions, themes, and a timeline of major cyber attacks and respective cyber sanctions programs;
- an overview of the legal framework as well as Office of Foreign Assets Control (OFAC) sanctions considerations, such as jurisdictional elements, potential penalties, prohibited payments, and facilitation risk;
- a number of high-level and in-depth case studies dealing with a variety of ransomware scenarios, examining responding to a ransomware incident, best practices, and regulator considerations in detail. Shorter versions of the case studies in the Masterclass have been adapted for use in this paper.

The Intersection of Ransomware and Sanctions Compliance

The US and a number of other governments generally discourage ransomware payments to criminal actors. Instead, organizations are encouraged to adopt policies and procedures aimed at reducing the risk of a successful attack in the first instance. While ransomware payments are not generally prohibited under legal frameworks, organizations will need to consider the risk of a ransomware payment violating economic sanctions, for example those in place in the US.

As such, organizations need to take OFAC sanctions risk into account in any ransomware incident, specifically in determining whether and under what circumstances they pay, process, facilitate or (in the case of insurance) indemnify a ransomware payment. Falling afoul in such an instance carries significant moral, reputational and enforcement risks to your organization.

The Advisory

To help organizations to mitigate their risk, in October 2020 OFAC published an *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* ("the Advisory"), elements of which will be emphasized throughout this briefing paper.[5] The Advisory encourages financial institutions (FIs) and other organizations to maintain a risk-based compliance programme which takes into account the risks of making ransomware payments to designated persons.

[5] Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (home.treasury.gov)

OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including those responsible for ransomware attacks and facilitating ransomware transactions.

Jurisdictional Risk

Organizations will also need to consider their jurisdictional risk when dealing with a ransomware attack and any subsequent payment. For instance, US primary sanctions apply to those with a US nexus, for example US persons as well as activities occurring within US territory. A US nexus can also include non-US entities conducting business in the United States, even if they are not physically present in the United States.

It is essential to understand your jurisdictional exposure and understand whether US sanctions apply to you. It is also important to keep in mind OFAC's concept of strict liability, meaning that even inadvertent and unintentional violations of sanctions can lead to civil penalties.

Masterclass Key Themes: Navigating the Nexus of Cyber, Ransomware and Sanctions Compliance

A helpful way of navigating this issue is to examine the different stages of a potential ransomware attack, including:

- Risk management/taking a risk-based approach before an attack;
- Incident management in the event of an attack;
- Factors to consider should payment be made to a sanctioned party;
- Licensing considerations.

It should also be noted that the predominant focus of the Masterclass and this briefing is with regards to OFAC sanctions risk.

Risk Management

It is essential that organizations determine their policies and procedures ahead of a ransomware incident occurring, to enable a quick, effective and compliant response.

A first step in considering your ransomware sanctions risk is to understand what your risk appetite is for a potential ransomware-related sanctions violation. This informs your risk-based approach as part of your sanctions compliance program.[6] Within the Advisory, OFAC encourages FIs and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations. This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services).[7]

[6] To assist the public in developing an effective sanctions compliance program, in 2019, OFAC published *A Framework for OFAC Compliance Commitments*, intended to provide organizations with a framework for the five essential components of a risk-based sanctions compliance program. The Framework is available at: https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf

[7] The Advisory, p.3

Policies and procedures are essential to a robust sanctions compliance program. Companies should ensure that their policies are clear as to whether, and under what circumstances, they will pay, process, facilitate, or insure a ransomware payment, and put in place adequate safeguards to reduce the risk of an attack.

From the FI perspective, a key risk which you must be prepared for is the scenario in which your client/customer asks you to process a ransomware payment on their behalf. Some general principles to consider in this situation include:

Governance
Robust governance processes are an important element in managing your ransomware risk. Questions to consider here include: who's going to decide whether to process a payment within your institution? And who are the key stakeholders? This should include financial crime professionals, but also potentially fraud deterrence, cyber security, risk officers and others. The formulation of a committee or task force can be key to help make that decision.

Documentation
It is essential that organizations have adequate documentation in place. This could include process outlines, risk appetite, relevant committees, escalation procedures, and even a detailed explanation of what ransomware is and scenarios of what ransomware payments tend to look like. In some cases, documentation may need to go further, and could outline the communication strategy and information management.

Audit
Ransomware and wider cyberattack risk should also be considered in the context of audit, for example whether audit is being appropriately adapted in terms of the financial crime review, i.e. in relation to regulatory advisories that have been issued.

An FI should also consider whether ransomware should be integrated into the enterprise-wide training plan and, if so, should identify which employees should receive the training.

Ransomware payments may also expose FIs to money laundering risk. That includes increased regulatory reporting obligations if the FI has reason to know or suspect that the financial institution is being used to facilitate criminal activity.[8]

The general principles of robust governance and documentation procedures are important for any organization – FI or otherwise – in managing its ransomware sanctions risk and informing its risk-based approach. Central to managing an incident of a ransomware attack is to have an effective incident response plan, including protocols which employees have been well trained in, undertaken test runs and will follow in the event of an attack.

Undertaking the above measures and asking these questions in advance enables organizations to respond quickly, with agility, to any incident. Furthermore, it ensures that documented evidence is there for regulators when they ask questions.

[8] See FinCEN Guidance, FIN-2020-A00X, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, October 1, 2020, for applicable anti-money laundering obligations related to financial institutions in the ransomware context.

Incident Management

If a ransomware attack occurs, it is critical that the victim undertake a number of steps to ensure management of OFAC sanctions risk. A first step is to follow the protocols outlined in your incident response plan.
The victim of the attack should also communicate and cooperate with law enforcement, as well as considering whether any suspicious transaction reports need to be submitted under relevant legislation. Furthermore, if the organization is weighing whether a ransomware payment should be made, all parties should take measures to ensure that the potential recipient is not a sanctioned person.

Communication with law enforcement

The Advisory outlines that one of the most important factors in assessing whether an enforcement action is needed, is whether the organization made a timely notification to law enforcement, and whether it cooperated with law enforcement both during and after the attack.[9] This is an extremely important part of any ransomware incident management framework.

It is also important to be aware of any suspicious transaction reporting requirements (for example if you are an FI potentially processing the payment). This may differ in different jurisdictions; you should be cognizant of local requirements.

Cryptocurrency and Ransomware

Cryptocurrency has been a common payment channel for ransomware payments and enhances the challenge of identifying criminals responsible for attacks, due to difficulties in attribution. After receiving the payment in a digital wallet, the funds would typically be moved and obfuscated as quickly as possible to avoid tracking and detection.[10]

Due diligence

While regulators and government authorities discourage ransomware payments, it is not generally legally prohibited - provided the recipient is not sanctioned under relevant legal frameworks. It should be noted that, across a number of jurisdictions, there is significant debate regarding whether ransomware payments should be outright banned, or stricter legislation introduced. However, as things currently stand, organizations which suffer a ransomware attack will need to decide whether they wish to pay the ransom and, if so, whether they legally can.

[9] OFAC encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus. Victims should also contact the US Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a US financial institution or may cause significant disruption to a firm's ability to perform critical financial services.
[10] Combatting Ransomware | A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force (securityandtechnology.org)

In determining whether a ransomware payment can be made, it is essential that victims, and other parties, conduct rigorous due diligence to understand whether the attacker is a sanctioned person, entity or parties acting on behalf of sanctioned jurisdictions (such as the DPRK government).
It can be beneficial to engage a cyber-incident response firm (CIRF).
A CIRF can undertake due diligence on the ransomware actor, for example through blockchain analysis, to try to determine – to the extent possible – whether payment is to be made to a sanctioned party. It can also help to ensure that the CIRF you are engaged with is registered as a money-service bureau, and is therefore subject to regulations itself. You will also need to determine whether you can accept the work undertaken by the incident response firm on your behalf, for example that it conforms to your standards of sanctions and AML procedures.

However, even undertaking as much due diligence as you possibly can, it is unlikely that you will be able to fully eliminate the risk of the recipient being a sanctioned party, and you may never know who is on the other end of the payment. FIs looking at processing the payment may have to decide whether to take that risk, depending on the information available, or to say no and risk their customer (the victim) potentially going out of business.

Case Study: IP Address

A US-based company has been the victim of a ransomware attack and is preparing to make the payment in the hope that its systems will be restored. Having done due diligence through a cyber incident response firm, it is found that the attacker, a group known as DarkSphere, share an IP address with an OFAC Specially Designated National (SDN), though no definitive connection has been established.

This significantly increases the risk of a potential violation of OFAC sanctions. Should the US-based company proceed with the ransom payment, it could face significant civil or even criminal liability.

Wider factors that may be relevant and will need consideration in how best to manage a ransomware demand include:

- What is the time and cost of restoring the systems and/or data without paying the ransom?
- What is covered under the insurance policy?
- Did you follow all the requirements to that coverage in the policy?
- Will you become more vulnerable to a future attack as a result of payment?
- The potential litigation and reputational risk linked to paying or not paying should be considered.
- Also consider what the objective of the attack is, and whether this has any bearing on the likelihood of systems and/or data actually being restored following payment.

Engaging with Your Insurer

Upon discovery of a ransomware incident, you may want to engage with your insurer in order to understand what coverage you have and what information they will need about the incident. You should consider:

- establishing out-of-band email (and regulatory compliant) communications to allow secure communications with key personnel, breach counsel, insurance brokers and insurers[11];
- working with insurers (or their appointed representatives) to retain qualified and experienced vendors providing specialist digital forensic and incident response (DFIR)/CIRF services, and specialist extortion services;
- some vendors offer both services while some offer one or the other – selection of a vendor should generally be made with insurers' prior written consent, whether given explicitly in response to a direct request, or from a panel of pre-approved vendors made available to the insured by insurers;
- preserving systems in consultation with a breach coach and DFIR/CIRF vendor.

A strong audit trail and documentation should be ensured throughout, to prove good governance and processes.

If Payment is Made to a Sanctioned Party

If an organization finds itself in a situation in which a ransomware payment has been made to what turns out to be a sanctioned party or person, the Advisory lays out the different factors that OFAC will consider in determining whether and what enforcement response is warranted.[12] These include:

- Did the entity have a risk-based compliance program?
- Did the entity make a self-initiated, timely, and complete report of the attack?
- Both during and after the attack, did the entity cooperate fully and in a timely manner with law enforcement?
- Did the entity ensure work done on its behalf, for example by a CIRF, met its sanctions and AML compliance standards?

While undertaking all of the above may reduce the likelihood of an enforcement action, it is impossible to guarantee that one would not be taken.

OFAC's *Economic Sanctions Enforcement Guidelines* provide more information regarding OFAC's enforcement of US economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation.[13]

[11] Email and messaging systems can be compromised in a ransomware attack. An out-of-band communication channel enables separate communication without relying on the potentially compromised system.
[12] The Advisory, p.3
[13] The Advisory, p.3

License Considerations

Sanctions programs generally provide certain exceptions under the financial sanctions and export control regimes. For instance, if relevant it may be possible to apply to OFAC for a specific license, allowing otherwise prohibited transactions to take place in certain circumstances. In the case of ransomware, the Advisory makes clear that, while a US person may seek a license from OFAC, there is a "general presumption of denial".[14] That said, it is possible to apply for an emergency specific license to make a ransomware payment to a sanctioned party, but such licenses will only have a chance of being granted on national security/foreign policy grounds.

If an emergency specific license application is submitted to OFAC, no payment should be made until this has been approved. Payment is only permitted in a case in which the organization becomes aware of new facts that give it certainty that the recipient is not connected to an SDN.

Case Study: Emergency Specific License

A US-based company which supplies electricity for domestic use has been the victim of a ransomware attack, and is concerned that it faces significant financial and reputational risks if its systems are not restored shortly. It decides that it needs to make the payment, but due diligence has revealed a number of red flags indicating that the recipient may be on the OFAC SDN list. The company applies for an emergency specific license on national security grounds. However, in the meantime, the hacking group states that it will begin leaking sensitive personal data if payment is not received in the next 24 hours.

Were the US-based company to make the payment while the license is still under consideration from OFAC, it would be extremely risky and looked at unfavourably by OFAC in the consideration of any enforcement response.

It should be noted that, from an OFAC perspective, it is not relevant whether the victim faces significant financial and reputational harm if no payment is made. While it should be considered in the organizations decision-making, it is important to be aware that it is not factored in to OFAC's license-making decision.

Other Jurisdictions' Sanctions Regimes

While the US has the largest cyber sanctions regime and has produced the most comprehensive advisory on ransomware, this is an international issue that is not specific to any single geographic location. It should be kept in mind that some cyber criminals, and other parties responsible for ransomware attacks, are sanctioned under other jurisdictions' sanctions regimes. This includes the UK and EU, with more designations expected in the future.

[14] The Advisory, p.4

This can present similar sanctions risks, dilemmas, and related questions to those which have been outlined in this paper. For example, the EU has sanctioned a number of individuals and entities responsible for ransomware attacks, such as those behind the 2017 WannaCry attack. As such, organizations should be aware of relevant prohibitions in other jurisdictions which need to be managed.

Summary

Key Takeaways from the Masterclass

The following key considerations stood out from the Masterclass:

1. It is important to consider ransomware sanctions risks within the context of your organization's sanctions compliance program.
2. Understand your risk-based approach – make sure the right people are involved and there are a clear set of decisions to make. Pay attention to red flags and mitigate the risks depending on the jurisdictions you are located in.
3. Ensure you build your program out, define your risk tolerance, do appropriate training and testing, and follow your procedures.
4. In considering making a ransomware payment, ensure you have done due diligence on the potential recipient.
5. If you engage with a cyber incident response firm, ensure it adheres to your standards of sanctions and AML procedures.
6. A strong governance framework and controls are important in a worst-case scenario, and are instrumental in advocating for why a civil or criminal response is not warranted.
7. Ensure you have a strong audit trail, so you can demonstrate that you have followed best practice to regulators.
8. When applying for an emergency specific license for ransomware, keep in mind OFAC's presumption of denial.

Conclusion and Looking Ahead

Ransomware is an issue which appears to be increasing in scope and scale. As such, it will continue to be a focus for regulators and government in the US and other countries.

There are many aspects involved in responding to ransomware attacks, which involve legal and reputational risks to victims, their banks, and insurers. It is also possible that we could see a move, by the US or other jurisdictions, to prohibit ransomware payments altogether. Regardless, OFAC will continue to impose sanctions on actors that materially assist, sponsor, or provide financial, material, or technological support to malicious cyber activities. It is important to keep up to date to ensure your organization is as protected as it can be.

ACAMS, in conjunction with the International Sanctions Compliance Task Force, will continue to work on ransomware in the context of sanctions compliance as a key area for further public-private cross-industry dialogue.

Furthermore, in the coming months ACAMS will be running a global survey on ransomware, the focus of which will include industry perceptions of threats and vulnerabilities, the extent to which ransomware sanctions risks are considered and prepared for, and areas in which industry would find further dialogue or guidance most useful.

About ACAMS

ACAMS is the largest global membership organization for anti-financial crime professionals, with 82,000+ members in over 175 countries/regions.

ACAMS offers two exclusive programs for sanctions professionals – the internationally recognized Certified Global Sanctions Specialist (CGSS) accreditation, and the Sanctions Compliance Foundations online certificate (new in 2021).

Also available to sanctions teams and professionals is the ACAMS Sanctions Space, led by Dr Justine Walker and our International Sanctions Compliance Task Force. The Sanctions Space is a comprehensive and dynamic resource center, encompassing Masterclasses, Global Monthly Update briefings, authoritative white papers and a podcast series telling the stories behind the sanctions.

Learn more about sanctions at ACAMS at **acams.org/sanctions**

Sam Cousins, Sanctions and Risk Associate, ACAMS

September 2021