Ransomware and Sanctions

Guidance on Ransomware and Financial Sanctions

HM Treasury
Office of Financial
Sanctions Implementation

Executive summary

- Ransomware is a significant threat to the UK. Ransomware payments to the criminal groups behind these attacks perpetuates the threat and does not guarantee victims will regain access to their data.
- His Majesty's Government (HMG) does not condone the making of ransomware payments.
- The National Cyber Security Centre (NCSC) provide guidance on cyber resilience measures that significantly reduce the risk and impact of a successful ransomware attack.
- If you have been subject to a ransomware attack, you should use HMG's Where to Report a Cyber Incident portal as soon as possible for direction on how to report your incident. Engaging with HMG will enable you to access support for managing your cyber incident.
- HMG has and will take strong action against ransomware threat actors, including the use of financial sanctions. Financial sanctions prohibit making funds or economic resources available to an individual or entity subject to an asset freeze, including through a ransomware payment.
- Breaches of financial sanctions are a serious criminal offence and can carry a custodial sentence and/or the imposition of a monetary penalty.
- The Office of Financial Sanctions Implementation (OFSI) assesses all breaches of financial sanctions on a case-by-case basis. OFSI will take several factors into account that will aggravate or mitigate when determining the facts and how seriously OFSI views a case.
- If the mitigating steps outlined in this guidance are taken, OFSI and the National Crime Agency (NCA) would be more likely to resolve a breach case involving a ransomware payment through means other than a monetary penalty or a criminal investigation.

Introduction

In recent years ransomware has evolved into a serious cybercrime threat to the UK. HMG seeks to disrupt and reduce the profitability of ransomware through using financial sanctions against the ransomware threat actors causing the highest harm to the UK.

Making or facilitating a ransomware payment risks exposing those involved to civil or criminal penalties where such payments are made to individuals or entities subject to financial sanctions, known as designated persons ("DPs"). These risks will be described in this guidance document along with advice for engaging with HMG, as well as aggravating and mitigating factors HMG will consider for any related civil or criminal enforcement action relating to financial sanctions breaches.

Background

Ransomware is a type of malicious software ("malware") that prevents victims from accessing their computer or the data that is stored on it until a ransom fee is paid. Some malware will also try to spread across a compromised network, such as the WannaCry malware that impacted the NHS in May 2017.[1]

Some cyber criminals are also known to use a double extortion methodology of both data encryption and data exfiltration; rather than just encrypting files, the double extortion tactic exfiltrates the data first which provides the threat actors leverage to threaten to sell and/or leak the data online if a victim refuses to pay the ransom demand.

Some cyber criminals, rather than encrypting before exfiltrating, will simply just exfiltrate all of the victim's data and then threaten to leak sensitive data or threaten to contact the victim's customers and associates identified in the exfiltrated data.

Victims will usually be asked to contact the attacker via an anonymous email address or to follow instructions on the dark web, to make payment in cryptocurrencies, in exchange for decryption to restore access to programs and data and avoid data being leaked online.

In the criminal marketplace, malware variants used for ransomware campaigns are in some cases offered as a purchasable service, in which a cyber criminal or group might sell or lease their ransomware for use by other criminal actors.

Impact of ransomware payments

Threat actors involved in ransomware attacks are motivated by financial profit from their criminality. Ransomware attacks against sectors, businesses and individuals are conceived in such a way to maximise the criminal ransom demanded within the victim's ability to pay.

Ransomware payments to criminal actors perpetuate the threat and sustain the criminal marketplace. Payment of a ransom further encourages the targeting of UK business and does not remove criminal actors' access to networks leaving them open to future attacks. This has a negative impact on UK national security and the economy and further encourages the targeting of UK individuals and entities.

The payment of a ransom does not guarantee a victim will regain access to their data or computer and increases the likelihood they will be targeted in the future. There are examples of payments resulting in decryptors not being provided or being faulty. There are also instances in which ransomware payments were made, files were decrypted, and the victim then suffered a further infection and ransomware demand from another actor that had utilised the same vulnerability or exploit.

HMG does not condone making ransomware payments and promotes the strengthening of cyber resilience measures to prevent and mitigate against ransomware attacks. Victims should report to and cooperate with HMG and law enforcement at the earliest opportunity.

Paying a ransom to a DP might also expose victims, and organisations facilitating ransomware

[1] NCSC, Mitigating malware and ransomware attacks.

payments on behalf of the victim, to liability for civil and criminal penalties.[2]

Cyber sanctions legislation

The UK has enforced financial sanctions under the Cyber sanctions regime since May 2019. The Cyber sanctions regime was originally introduced when the UK was part of the European Union ("EU"). Following the UK's exit from the EU, the Cyber (Sanctions) (EU Exit) Regulations 2020 ("the Regulations") were introduced under the Sanctions and Anti-Money Laundering Act 2018.

The Regulations are aimed at, among other things, furthering the prevention of cyber activity which undermines, or is intended to undermine, the integrity, prosperity or security of any country, including the UK; directly or indirectly causes economic loss to, or prejudice to commercial interests of, those affected; or undermines, or is intended to undermine, the independence or effective functioning of an international organisation or a non-governmental organisation or forum whose mandate or purposes relate to the governance of international sport or the internet.

The Regulations provide for the imposition of asset freezes and travel bans on persons involved in relevant cyber activity as defined in defined in Regulation 4 of The Cyber (Sanctions) (EU Exit) Regulations 2020 Under an asset freeze, it is prohibited for a person to make funds or economic resources (including cryptoassets), available directly or indirectly to, or for the benefit of, a DP. Intentionally participating in activities that circumvent, or enable or facilitate the contravention of, the financial sanctions prohibitions in the Regulations is also prohibited.

Breaches of financial sanctions are a serious criminal offence. OFSI has the power to impose civil monetary penalties for breaches of financial sanctions under powers in the Policing and Crime Act 2017. The statutory maximum penalty OFSI may impose is the greater of £1 million or 50% of the value of the breach (which may be estimated).

Although OFSI has the power to issue monetary penalties for breaches of financial sanctions, many of its cases are dealt with through other means. Other steps OFSI takes in response to a breach include issuing a warning, referring regulated entities to their relevant professional body or regulator, or publishing information pertaining to the breach.

The UK government does not encourage or condone ransomware payments, whether you are dealing with a DP or not.

Sectoral sanctions risk

As well as asset freezes, some regimes have sectoral sanctions which prohibit and restrict specified activity. Sectoral sanctions may include restrictions on the transfer of funds to or from a jurisdiction. Facilitating a ransomware payment may breach UK sectoral sanctions, or the law of other jurisdictions. HMG has produced guidance on each sanctions regime that gives details of sectoral sanctions.

HMG's approach to enforcement and what you need to do

Due diligence

In order to mitigate the risks of a financial sanctions breach, NCSC's preventative cyber resilience measures (see "Cyber resilience and mitigating ransomware attacks" below) and effective due diligence measures can be implemented by individuals and entities.

Financial sanctions are widely publicised and businesses, particularly those operating internationally, should routinely consider whether sanctions might affect their transactions. Each organisation should assess its own exposure and put due diligence measures in place to manage any identified or anticipated risks of breaching financial sanctions.

OFSI does not mandate specific financial sanctions systems or controls or due diligence measures. OFSI cannot provide legal advice and the onus is on the organisation to ensure it has put in place sufficient measures to avoid committing a breach of financial sanctions. This also applies to persons that engage with victims of ransomware attacks

[2] Persons involved in facilitating could be, but are not limited to, financial institutions, cryptoasset businesses, cyber insurance and cyber incident response companies.

including any person or entity that facilitates or processes ransomware payments.

Reporting a ransomware incident

If you have been subject to a ransomware attack, you should use HMG's Where to Report a Cyber Incident portal as soon as possible to be directed to the correct organisations to which to report your incident.

You will be guided through a series of questions on the portal, for a ransomware incident it will direct you to Action Fraud, which is the UK's reporting centre for fraud and cybercrime in England, Wales and Northern Ireland. Those in Scotland will be directed to Police Scotland. You may also be directed to the NCSC, part of the Government Communications Headquarters (GCHQ), the UK's technical authority for cyber threats.[3] You should report your ransomware-related cyber incident to these authorities if prompted by the Where to Report a Cyber Incident portal. As part of its role NCSC, in partnership with the NCA and police forces, may provide incident response support to those affected by cyber incidents.

Cooperation with OFSI and law enforcement

OFSI is the authority responsible for implementing the UK's financial sanctions on behalf of HM Treasury. OFSI is responsible for monitoring compliance with financial sanctions, for assessing suspected breaches of financial sanctions, and for referring appropriate cases to law enforcement partners for criminal investigation and potential prosecution.

If you suspect a ransomware payment has been made to a designated person, you should report this to OFSI as soon as practicable. A prompt and complete voluntary disclosure of a breach of financial sanctions by a person who has committed a breach will generally be a mitigating factor when OFSI assesses the case and any potential enforcement action.

Each suspected breach is treated on its own merits and all the facts are assessed in each case to decide an outcome that is proportionate. OFSI will take several factors into account that will aggravate or mitigate when determining the facts and how seriously OFSI views a case. Aggravating factors may include regulatory standards not being complied with by regulated professionals and or repeated, persistent or extended breaches by the same person.

Where a ransomware payment has been made to a DP by a victim, OFSI will generally consider as mitigating factors, both the ransomware incident being reported by the victim to the relevant organisations through the Where to Report a Cyber Incident portal, and a prompt and complete voluntary disclosure of the payment to OFSI as soon as practicable. In OFSI's assessment of cooperation with NCSC and law enforcement, OFSI will consider if there was engagement with law enforcement both during and after a ransomware attack, and whether all relevant information, including technical details, information on the ransom payment and accompanying instructions, was provided.

Where a ransomware payment to a DP has been facilitated by a third party (such as a financial institution or cryptoasset business), OFSI will generally consider as a mitigating factor for the third party, a prompt and full voluntary disclosure made to OFSI as soon as practicable.

OFSI may refer breaches of financial sanctions to the NCA for further investigation where this is appropriate. An investigation by the NCA is very unlikely to be commenced into a ransomware victim, or those involved in the facilitation of the victim's payment (which could include but is not limited to financial institutions, cryptoasset businesses, cyber incident responders, insurance and negotiating service providers), who has proactively engaged with the relevant bodies as set out in the mitigating factors above.

In the event an NCA investigation concluded there was sufficient evidence and it was in the public interest, the final decision to pursue a criminal prosecution for breaches of financial sanctions ultimately lies with the prosecuting authorities. Details would be passed to the Crown Prosecution

[3] When supporting victims, NCSC can provide technical advice and guidance, use its unique access to information as part of GCHQ to help the victim understand the incident better, coordinate any cross-government response and help with public communications.

Service (CPS) who would independently decide whether there was (i) sufficient evidence to prosecute and (ii) a prosecution was required in the public interest. The assessments of evidence and public interest are taken in accordance with the Code for Crown Prosecutors.

If the mitigating steps outlined above are taken, OFSI and the NCA would be more likely to resolve a breach case involving a ransomware payment through means other than a monetary penalty or criminal investigation.

How do I know if I am dealing with a designated person?

The Foreign, Commonwealth and Development Office's UK Sanctions List contains identifying information about the individuals, entities and ships designated under regulations made under the Sanctions and Anti-Money Laundering Act 2018.

OFSI's Consolidated List contains identifying information about the designated persons subject to an asset freeze in the UK as a result of UN and UK sanctions. The list provides information to help you decide whether you are dealing with someone who is subject to sanctions.

An asset freeze will apply to funds and economic resources of entities that are owned or controlled, directly or indirectly, by a DP.[4] The prohibitions on making available funds or economic resources will also extend to entities that are owned or controlled, directly or indirectly, by a DP. Those entities may not be designated in their own right, so their names may not appear on the Consolidated List or UK Sanctions List. However, those entities are similarly subject to financial sanctions.

It is up to all individuals and organisations to ensure that they are not making funds or economic resources available to or for the benefit of a DP. Neither OFSI nor the NCA mandate the use of particular financial sanctions systems or controls. Regulated professionals should meet regulatory and professional standards.

Can I apply for a licence?

A licence is a written permission from OFSI authorising an act that would otherwise breach financial sanctions prohibitions. OFSI can only issue specific licences where there are specific and relevant licensing grounds in the enabling legislation and where the conditions in those grounds have been met. The available grounds

can be found in legislation underpinning each particular financial sanctions regime.

OFSI reviews licence applications on a case-by-case basis. Ransomware payments are unlikely to be considered appropriate for an OFSI licence. You should consider seeking independent legal advice before applying.

Victims of ransomware attacks

HMG strongly encourages all victims, and those engaging with victims, to report ransomware incidents to Action Fraud or Police Scotland and NCSC. HMG closely monitors and investigates ransomware-related criminal activity and may uncover an unreported ransomware payment to a DP.

A ransomware attack involving the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data may be a breach of UK General Data Protection Regulation or the Data Protection Act 2018. You may be required to report the breach to the Information Commissioner's Office (ICO).

Dealing with a ransomware attack

The below are steps that should be considered when dealing with a ransomware attack. This is not an exhaustive list and good judgement should be exercised.

- Disconnect the infected device from all network connections, whether wired, wireless or mobile phone based.
- Use HMG's Where to Report a Cyber Incident to be directed to the correct organisations to report the ransomware attack and demand for ransom as soon as possible.

[4] Entities meaning a body of persons corporate or unincorporate, or any organisation or association or combination of persons

- Implement effective due diligence to mitigate the risks of a financial sanctions breach, which may include but is not limited to attempting to restore from back-ups resulting in no need to consider a payment.
- Consider that you may need to comply with another jurisdiction's requirements. You should check whether you are dealing with an individual, entity or country which is subject to sanctions under another jurisdiction.
- Submit a report to the ICO if a breach under the UK GDPR or Data Protection Act 2018 has occurred.
- If applicable, report the incident to your sector's regulator to fulfil any applicable regulatory obligations you might have.
- Seek independent legal advice where necessary.

Cyber resilience and mitigating ransomware attacks

NCSC's advice and guidance, if implemented, would drastically reduce the risk of a successful ransomware attack. Relevant Active Cyber Defence capabilities serve to further reduce that risk. NCSC provide a guide to understanding ransomware and advice on how to protect against ransomware attacks.

The NCSC runs an assurance scheme called Cyber Incident Response. Members of this scheme meet the NCSC's standard for high quality incident response to affected organisations.

Exercise in a Box is an online tool from NCSC which helps organisations understand their resilience to cyber attacks, by allowing you to test and practice your response to an cyber attack.

Early Warning is a free service provided by NCSC, designed to inform your organisation of threats against your network.

Boards are pivotal in improving the cyber security of their organisations. NCSC has produced the Cyber Security Toolkit for Boards, for Board members to get to grips with cyber security.

The Small Business Guide: Response and Recovery and the Small Charity Guide is advice produced by NCSC to help small businesses and charities protect themselves from the most common cyber attacks.

Rebuilding after a ransomware incident: section 6 of NCSC's guidance provides advice for responding and recovering from ransomware.

Consider whether your organisation would benefit from cyber insurance. Guidance for considering cyber insurance has been provided by NCSC.

Contacts

For reporting a ransomware attack (ongoing and past), you must use HMG's Where to Report a Cyber Incident portal: www.gov.uk/guidance/where-to-report-a-cyber-incident.

For reporting a breach under UK GDPR or the Data Protection Act 2018 please report to: https://www.ico.org.uk/global/contact-us.

For further information on financial sanctions: contact OFSI ofsi@hmtreasury.gov.uk or subscribe to OFSI's email alerts https://public.govdelivery.com/accounts/UKHMTREAS/subscriber/new.

If you suspect a breach of financial sanctions has occurred, please report to OFSI: https://www.gov.uk/guidance/suspected-breach-of-financial-sanctions-what-to-do.

OFSI's consolidated list of asset freeze targets can be found here: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.

OFSI's general guidance for financial sanctions can be found here: https://www.gov.uk/government/publications/financial-sanctions-faqs

For general information on sanctions: contact the Foreign, Commonwealth & Development Office's Sanctions Directorate on sanctions@fcdo.gov.uk.

The UK Sanctions List can be found here: https://www.gov.uk/government/publications/the-uk-sanctions-list.