LLOYD'S

Market Bulletin

Ref: Y5359

Title	**Guidance for handling a ransomware claim incident**
Purpose	To inform the market of matters to consider when assessing ransomware claims
Type	Event
From	Chris Po-Ba Senior Manager Financial Crime Advisory (Market)t: +44 (0)20 7327 5473
Date	10 December 2021
Deadline	
Related links	**Appendix 1**

This market bulletin provides guidance to managing agents for handling ransomware incidents impacting an insured or reinsured. This guidance has been produced in conjunction with London market insurers and brokers, the Lloyd's Market Association (LMA) and industry experts. This guidance is general in nature and does not override specific laws and regulations that may apply. It also does not deal with ascertaining coverage. Where appropriate, legal advice should be obtained.

See **Appendix 1** for specific guidance aimed at Market Participants' Legal, Compliance and Claims functions, for the handling of a ransomware incident.

Background

In recent years, ransomware attacks have become increasingly frequent as a way of extracting funds. Ransomware is a computer virus that disables computers and encrypts systems and files so that the affected entity cannot view or access those files. The cyber-criminal then demands a ransom, usually via a pop-up box, in exchange for a decryption key to restore systems and decrypt impacted files. Victims of ransomware attacks also increasingly face secondary extortion schemes, where cyber criminals threaten to publish or sell data stolen from their systems. These ransom demands usually require payment in Bitcoin or other cryptocurrency.

There are additional complications for the victim and anyone facilitating payment of a ransom, including the victim's insurers, if a ransom payment is made to, or involves, a designated person, entity, region or country, or virtual currency exchange, wallet or malware variant that is subject to sanctions (together a "sanctioned party").

In recognition of this threat, cyber-related sanctions regimes have been implemented by various states to complement existing anti-money laundering and counter-terrorist frameworks.

Financial crime and sanctions risks

Before any payment or reimbursement of an insured is made managing agents need to consider whether payment is permitted to be made and whether any notification is necessary. This requires awareness of, or advice relating to, the following in all applicable jurisdictions (and at a minimum where the insured and managing agent are located):

- Anti-money laundering (AML) laws and regulations;
- Counter-terrorism laws and regulations;
- Sanctions laws and regulations, including, where applicable, US secondary sanctions and non-US 'Blocking Statutes'; and
- Suspicious activity laws and regulations as applicable to industry including any required notifications to authorities.

Managing agents should have systems and controls in place to mitigate the following risks:

- Facilitating a transaction which involves a sanctioned party or is linked to terrorism;
- Failing to disclose suspicion or other information to relevant authorities where required[1];
- Inaccurately disclosing an incident to relevant authorities; and
- Failing to implement adequate controls.

Claims Agreement Parties (Lloyd's)

In the event of a ransomware claim being notified to managing agents, and in advance of a potential ransom payment being made, the Claims Agreement Party(ies) should inform all managing agents on the contract to allow those parties to consider in advance whether they have any different obligations arising due to where they are domiciled and how their ownership is structured, and to initiate processes and checks as part of their sanctions controls and compliance framework.

The Claims Agreement Party(ies) should refer to the Lloyd's Claims Schemes' financial and non-financial considerations. This will be relevant to triaging the ransomware claim and ensuring that the Claims Agreement Party(ies) are making appropriate and early arrangements to inform subscribing insurers of the claim and potential payment.

Delegated Authority Arrangements

Where managing agents delegate claims handling authority to a Third-Party Administrator (TPA), the due diligence and oversight process will set the controls for the management of claims by the TPA. This should include the due diligence on ransomware claims, if the TPA will be handling such claims. A copy of this guidance should be appended to the third party or Delegated Claims Handling Agreement (LMA9188) with the stipulation that such guidance must be followed and that managing agents need to be notified in advance of any payment

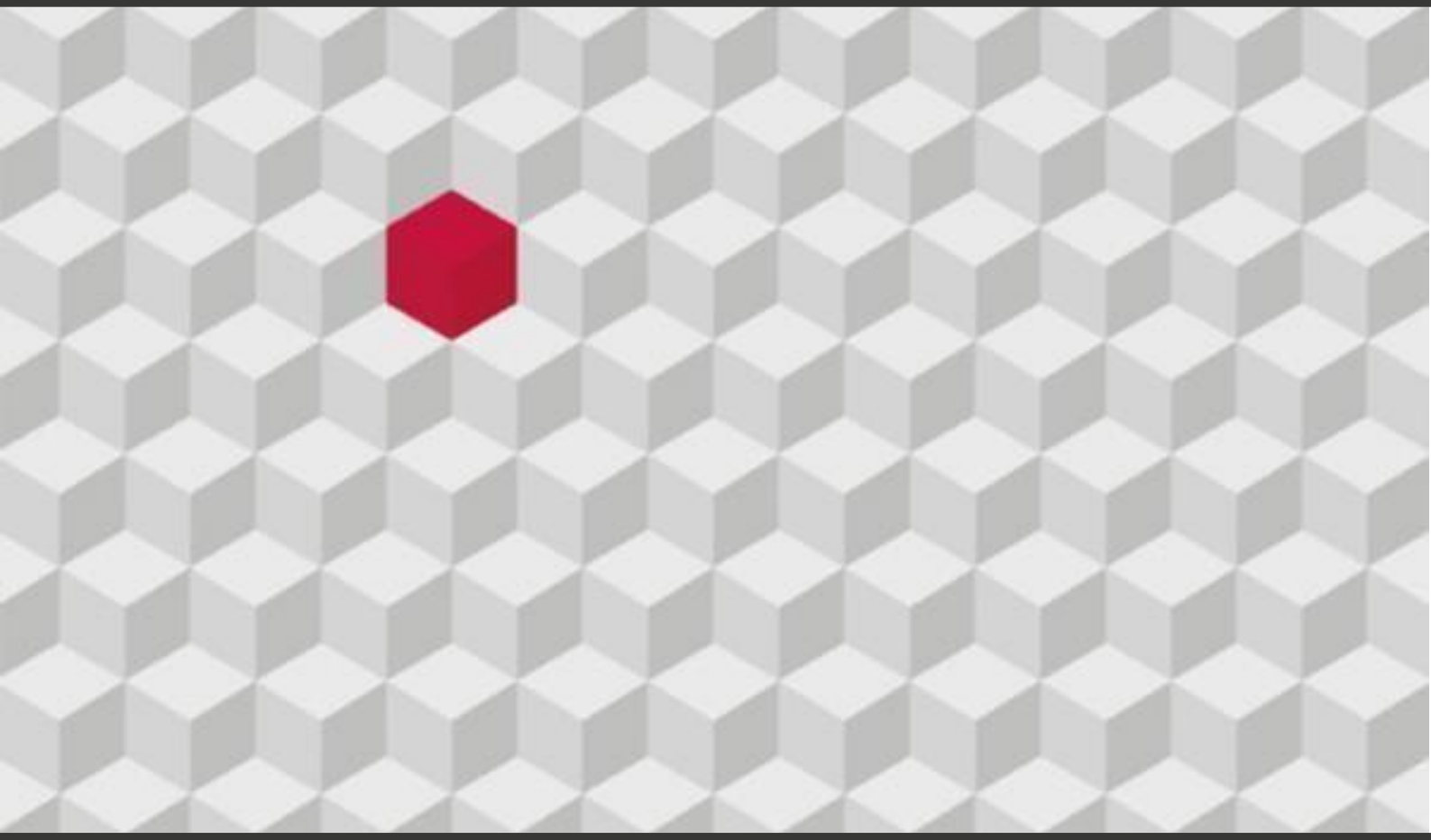
[1] For example, in the UK, Suspicious Activity Reports (SARs) under Proceeds of Crime Act 2002 (POCA).

to ensure that, if necessary, they are able to follow processes and checks as part of their sanctions controls and compliance framework.

Contacts

For further information please contact:

- **Arabella Ramage** (Legal Director – LMA) – arabella.ramage@lmalloyds.com
- **Shanaz Ferreira-Cooper** (Technical Executive – LMA) – shanaz.ferreira-cooper@lmalloyds.com



Guidance for handling a ransomware incident

Facilitating a better future

lmalloyds.com

Contents

The Guidance has been produced in conjunction with London market insurers and brokers, the Lloyd's Market Association (LMA) and industry experts. It is intended to provide guidance to insurers for handling ransomware incidents impacting an insured. The guidance is general in nature and does not override specific laws and regulations that may apply. It also does not deal with ascertaining coverage. Where appropriate, legal advice should be obtained.

Regulatory engagement

Relevant laws and regulations will vary by country. Addressing all relevant jurisdictions is outside the scope of this guidance. Some key considerations are set out below, although the current position in any relevant jurisdiction should always be confirmed.

Anyone involved in responding to, or facilitating a response to, a ransomware attack should have robust risk-based compliance programs and protocols in place to avoid breaching sanctions.

Insurers will have to consider in each case the rules that apply to them because of the following:

1. Who is handling the claim;
2. Who owns the insurer; and
3. Where the insured is located.

Steps taken by insureds to maximise cyber resilience, showing investment in security and training in related areas, plus an open dialogue with regulators in the event of a ransomware incident, may help mitigate exposure to sanctions violations.

It is imperative to document each step of the due diligence process. This may be critical in any dialogue or proceedings with regulators to demonstrate compliance with AML requirements and sanctions. It will also assist insurers when considering requests for consent to any payment being made, if required by policy conditions.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) have each released advisories addressing financial crime and sanctions related risks associated with ransomware and ransomware payments.[1]

The OFAC Advisory states that "Meaningful steps taken to reduce the risk of extortion, such as those highlighted in the Cyber Security and Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide[2], will be considered a significant mitigating factor in any OFAC enforcement response". The Advisory indicates that mitigation in an enforcement response may be achieved by reporting ransomware attacks to CISA, the local FBI field office, the FBI Internet Crime Complaints Center, or the local US Secret Service office as soon as possible.

The due diligence processes

The following sections of this guidance are intended for communication by insurers to the insured and/or the incident response vendors assisting the insured in navigating the ransomware incident. Insurers may consider that the type of guidance below should be included in the policy. The guidance assumes that coverage is on a reimbursement basis and that the ultimate decision as to whether to pay the ransom rests with the insured.

[1] *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, Department of the Treasury (September 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf. This Advisory updates and supersedes OFAC's prior Advisory, dated October 1, 2020.

See also the Financial Crimes Enforcement Network (FinCEN) Advisory dated October 1, 2020: https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

[2] See https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf and https://www.cisa.gov/stopransomware/ive-been-hit-ransomware.

a) Upon discovery of a ransomware incident, insurers should require an insured to do the following:

- Document each step of the due diligence process to demonstrate compliance with AML requirements, counter terrorism requirements and sanctions. It will also assist insurers when considering requests for consent to any payment being made, if required by policy conditions;
- Establish out-of-band email (and regulatory compliant) communications to allow secure communications between and with key personnel, breach counsel, vendors, insurance brokers and insurers (or their appointed representatives);
- Work with insurers (or their appointed representatives) to retain qualified and experienced vendors providing specialist Digital Forensic and Incident Response (DFIR) services, and specialist extortion services. Some vendors offer both services while some offer one or the other.
    - Selection of a vendor should 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.
    - In circumstances where a pre-approved panel vendor is not available and insurers (or their appointed representatives) cannot be reached (e.g. out of hours), any vendor selected by the insured should be asked to confirm that they are sufficiently experienced and able to assist the insured in taking the important steps outlined below.
- Preserve systems in consultation with a breach coach and DFIR vendor.

b) Before engaging in negotiations insurers should require an insured to:

- Comply with any mandatory requirements to notify law enforcement or relevant regulators;
- Consider whether it is appropriate to file an Internet Crime Complaint with the IC3 or a Suspicious Activity Report (SAR), or equivalent report dependent upon jurisdiction;
- Recognise that early engagement, transparency and cooperation may assist in identifying/tracking the cyber-criminal and provide a level of protection to an insured (and those facilitating any payment), should a payment later be identified as having been made to, or which involves, a designated person, entity, region or country, or virtual currency exchange, wallet or malware variant that is subject to sanctions (together a "sanctioned party");
- Consider whether to engage with the cyber-criminal with the knowledge of law enforcement, any relevant regulators and vendors experienced with the specific cyber-criminal where they can be identified;
- Consider the extent of encryption and whether it has affected back-ups;
- Consider whether viable back-ups are intact and sufficient to restore critical systems, data and operations and estimate how long this is likely to take;
- Consider the overall impact on the insured's systems, operations and business;
- Consider whether data has been exfiltrated and, if so, the type of data at risk and the potential problems associated with its publication (data concerns should be discussed with breach counsel);
- Secure evidence from the forensic investigation relevant to the decision whether to make the ransom payment;
- Secure the environment (containment);
- Establish a strategy for any anticipated negotiations - consider the goal of negotiating (e.g. obtaining decryption key; avoid having data leaked, stalling while achieving containment, obtaining information helpful to DFIR vendors for determining scope of the investigation).

c) Due diligence process expected of an insured who anticipates making a ransom payment:

Any decision by the insured to make a ransom payment should only be taken after consideration of the following:

- Have other avenues been exhausted?
- Is payment lawful?
- Is there any other compelling reason not to pay?
- Does the payment require consent of the insurer, vendor, an executive of the insured, or any other party?

If, at any step of the process, any results are returned that establish an actual or suspected link with a sanctioned party, or that give rise to AML or counter-terrorism concerns, then prior to payment next steps should be discussed in conjunction with the vendor(s) and breach counsel, including what further consultation with law enforcement, any relevant regulator or insurers is required.

Prior to payment the steps an insured should follow (with the assistance of the appointed incident response vendors) are:

Block Chain Analysis:

1) Run the recipient cryptocurrency wallet ID/address or any associated cryptocurrency wallet ID/address through the lists maintained by the relevant government agencies responsible for the enforcement of economic and trade sanctions ("Enforcement Agencies") for the jurisdiction(s) concerned;
2) Run blockchain analysis to assess all transactions or wallets associated with the recipient cryptocurrency wallet ID:
    a. Historical cross-reference of wallet to linked wallet associations with respective Enforcement Agencies;
    b. Review historical transactions linked to the wallet;
    c. Identify past ransoms paid; and

3) Check the wallet ID against any other databases accessible to the vendor(s) engaged in assisting the insured with the ransomware attack.
4) To the extent possible, run the virtual currency exchange(s) used in the transaction through the lists maintained by the relevant Enforcement Agencies for the jurisdiction(s) concerned;

Threat Intelligence:

5) Cross reference tactics of the cyber-criminal, techniques, and procedures (TTPs) and other unique identifiers (such as IP addresses and domain names) against lists maintained by relevant Enforcement Agencies and internal intelligence databases;
6) Run ransomware variant name through Open-Source Intelligence and internal databases to identify information and intelligence from community and government sources;
7) Run the ransomware variant name and any associated malware/campaigns through lists maintained by relevant Enforcement Agencies.

Additional Precautions:

8) Verify that the cyber-criminal is real and credible:
    a. Is the cyber-criminal able to respond (internet connectivity, live person)?
    b. Is the cyber-criminal able to provide decryption key(s) that work (sample files decrypted)?
    c. Did the cyber-criminal exfiltrate any data (sample files, help determine scope of systems involved, help to determine legal obligations)?
    d. Weigh risk of re-extortion (historical data from vendors or law enforcement, atypical demands, any other warning signs).

Consent:

When an insured seeks reimbursement or consent from insurers to make a ransom payment, the insured will be expected to provide the following confirmation that, after having undertaken such due diligence as the circumstances allow, they have:

a. considered any mandatory requirements to notify law enforcement or relevant regulators; and
b. have no reasonable cause to believe that the ransom payment will be made to a terrorist or terrorist organisation or to further a terrorist purpose; and
c. have carried out sanctions checks against the lists maintained by relevant Enforcement Agencies; and
d. have no reasonable cause to believe that the ransom payment is being made to any sanctioned party.

Sufficient information should be provided to insurers to enable insurers to consider any obligations they may have under applicable laws and regulations, including any obligations they have to notify relevant Enforcement Agencies.