PRIVILEGED AND CONFIDENTIAL
SUBJECT TO ATTORNEY-CLIENT PRIVILEGE

[Date]

[Client Name]
[Client Address]
[City, State, Zip Code]

Re: Legal Advisory Regarding Ransomware Extortion Demand and Potential Payment

Dear [Client Contact Name],

This letter provides our formal legal advice regarding the ransomware demand issued by the threat actor identified as [Threat Actor Name/Group] following the cybersecurity incident discovered on [Date].

1. Sanctions Compliance and OFAC Search
We have conducted a screening against the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list. Based on our current intelligence, the threat actor [is / is not] explicitly named as a sanctioned entity. However, please be advised that payment to unidentified actors carries inherent risks of "indirect" sanctions violations if the funds are later traced to a prohibited jurisdiction or entity.

2. Law Enforcement Coordination
In accordance with FBI and Department of Justice guidelines, we strongly recommend that this incident be reported to the Internet Crime Complaint Center (IC3). Law enforcement generally discourages payment, as it does not guarantee data recovery and may encourage future attacks. However, they recognize that payment is a business decision based on the criticality of operations.

3. Legal Risks and Considerations
The primary legal risks associated with facilitating a ransom payment include:
- Potential violation of Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulations.
- No legal guarantee that the threat actor will provide a functional decryption key or delete exfiltrated data.
- Potential for additional extortion attempts following the initial payment.

4. Recommendation
If [Client Name] determines that the recovery of data is essential to the survival of the business and no viable backups exist, we advise that the payment be facilitated through a third-party Ransomware Negotiation firm to ensure proper documentation, proof-of-life for files, and secure cryptocurrency handling.

5. Documentation
Should you choose to proceed with payment, we must document the "necessity" of the payment to mitigate potential regulatory scrutiny. This includes documenting the failure of backups, the threat to life or safety, and the estimated economic impact of prolonged downtime.

Please confirm your instructions regarding how you wish to proceed with the threat actor negotiations.

Sincerely,

[Partner Name]
[Law Firm Name]