[Law Firm Letterhead]

[Date]

[Client Contact Name]
[Client Company Name]
[Address Line 1]
[City, State, Zip Code]

RE: LEGAL ADVISORY REGARDING RANSOMWARE EXTORTION PAYMENTS

Dear [Client Contact Name],

We are providing this advisory to outline the critical legal risks and regulatory obligations associated with making ransom payments to cyber-extortionists. In the event of a ransomware attack, your organization must consider the following legal frameworks before authorizing any payment.

1. Sanctions Compliance and OFAC Regulations
The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has issued advisories stating that paying a ransom to entities or individuals on the Specially Designated Nationals (SDN) list-or those located in sanctioned jurisdictions-is a violation of federal law. Strict liability applies, meaning a company can be penalized even if it did not know the recipient was a sanctioned party.

2. Anti-Money Laundering (AML) and Counter-Terrorism Financing
Facilitating payments to criminal organizations may trigger scrutiny under the Bank Secrecy Act and other AML statutes. Organizations must ensure that any payment does not inadvertently support terrorism or organized crime, which can lead to severe criminal prosecution.

3. Reporting Obligations
Depending on your industry and jurisdiction, you may be legally required to report the incident to the FBI's Internet Crime Complaint Center (IC3), the Cybersecurity and Infrastructure Security Agency (CISA), or specific sectoral regulators. Timely cooperation with law enforcement is often considered a mitigating factor if a sanctions violation occurs.

4. Fiduciary Duties and Insurance Considerations
Board members and officers must act in the best interest of the corporation. While paying a ransom may seem necessary for business continuity, it must be balanced against the risk of legal penalties. Furthermore, many cyber insurance policies have strict requirements for "consent to pay" and may deny coverage if legal due diligence is not documented.

5. Data Breach Notification Laws
Paying a ransom does not waive your legal obligation to notify affected individuals, regulators, or state Attorneys General if personally identifiable information (PII) or protected health

information (PHI) has been compromised. A "promise" from a hacker to delete stolen data is not legally sufficient to bypass notification requirements.

Conclusion
We strongly recommend that any decision regarding a ransom payment be made only after a forensic identification of the threat actor and a formal legal risk assessment. Please contact us immediately should you suspect a breach so we can assist in coordinating with law enforcement and regulatory bodies.

Sincerely,

[Partner Name]
[Law Firm Name]