[Date]

RE: Advisory on OFAC Compliance and Ransomware Extortion Risks

Dear **[Executive Name/Board of Directors]**,

This letter serves to formally advise **[Organization Name]** regarding the legal and financial risks associated with ransomware extortion payments, specifically concerning the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury.

1. Regulatory Framework
Under the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA), U.S. persons are prohibited from engaging in transactions with individuals or entities on the Specially Designated Nationals and Blocked Persons (SDN) List. This includes specific cyber-threat actors and state-sponsored groups.

2. Strict Liability Standard
OFAC applies a "strict liability" standard. An organization may be held civilly liable for a sanctions violation even if it did not know or have reason to know it was dealing with a prohibited party. This is particularly relevant in ransomware cases where attackers often use aliases or obfuscate their identity.

3. Potential Penalties
Violations can result in significant civil administrative penalties and criminal prosecution. Beyond financial fines, the reputational damage and potential loss of banking relationships present a material risk to the organization.

4. Recommended Response Protocol
In the event of a ransomware attack, the organization should adhere to the following OFAC-aligned steps:

- Immediate notification of the FBI or CISA.
- Verification of the attacker's identity against Sanctions Lists.
- Documentation of all due diligence efforts to mitigate potential penalties.
- Consultation with legal counsel before any payment is authorized.

5. Mitigating Factors
According to the "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," OFAC considers early reporting to law enforcement and robust cybersecurity posture as significant mitigating factors in any enforcement action.

Please acknowledge receipt of this advisory. We recommend incorporating these guidelines into the organization's Incident Response Plan (IRP).

Sincerely,

[Your Name/Signature]
[Your Title]
[Organization Name]