

[Date]

[Vendor Contact Name]
[Vendor Company Name]
[Address]

Subject: Advisory Regarding Ransomware Payment Risks and Compliance

Dear [Vendor Contact Name],

We are writing to you as a valued business partner of [Your Company Name] to address the evolving security landscape regarding ransomware and the associated legal and financial risks of making extortion payments.

In the event that [Vendor Company Name] experiences a ransomware incident that impacts the services provided to us or involves our data, we wish to formally communicate our position regarding ransom payments:

- **Regulatory Compliance:** We remind our partners that paying ransoms to entities on restricted lists (such as OFAC's Specially Designated Nationals list) may violate international sanctions and lead to severe legal penalties.
- **Verification Requirements:** Before any payment is considered or made, we require immediate notification and a full forensic report confirming that the threat actor is not an entity subject to government sanctions.
- **Data Integrity:** Research indicates that payment does not guarantee the recovery of data or the prevention of future leaks. We encourage a strategy focused on robust backup restoration and law enforcement engagement.
- **Reporting Obligations:** Per our contractual agreement, any breach involving our data must be reported to [Your Company Name] within [Number] hours, regardless of whether a ransom is being negotiated.

We strongly advise [Vendor Company Name] to maintain comprehensive cyber insurance and an incident response plan that prioritizes containment and recovery over extortion compliance.

Please acknowledge receipt of this advisory and provide a contact point for your Information Security team should we need to discuss your current ransomware mitigation protocols.

Sincerely,

[Your Name]
[Your Title]
[Your Company Name]