To: Board of Directors, Flair Airlines

From: Brian F. Smith

Date: 3 May 2024

Subject: Review of Federal Laws Relevant to Cybersecurity and Incident Disclosure

In light of the recent cybersecurity incident involving Flair Airlines' web server at https://flyflair.com, it's crucial to review the federal laws relevant to cybersecurity that could impact the company's liability to customers, shareholders, and potential fines/penalties from the government:

- **HIPAA** (Health Insurance Portability and Accountability Act): Flair Airlines is not directly subject to HIPAA regulations as it is not a healthcare provider or covered entity. Therefore, there is no liability to customers or fines/penalties from the government under HIPAA.
- **GLBA** (Gramm-Leach-Bliley Act): Flair Airlines, being an airline company, is subject to GLBA regulations concerning the protection of consumers' personal financial information. The compromise of sensitive customer data could lead to liability to customers and potential fines/penalties from the government.
- **SOX** (Sarbanes-Oxley Act): Flair Airlines, as a publicly traded U.S. company, is subject to SOX regulations. The compromise of sensitive data could impact financial reporting accuracy and potentially lead to liability to shareholders and fines/penalties from the government.
- **GDPR** (General Data Protection Regulation): While GDPR is an EU regulation, it applies to Flair Airlines if it processes personal data of EU citizens. Non-compliance could result in significant fines and liabilities to customers.

Liability and Fines/Penalties Assessment

- **Customers:** Flair Airlines would be liable to customers under GLBA and potentially GDPR for the compromise of personal information, including names, emails, and flight details.
- **Shareholders:** Shareholders may hold the company liable under SOX if the incident impacts financial reporting accuracy or poses financial risks to the company.
- **Government:** The government could impose fines/penalties under GLBA, SOX, and potentially GDPR for non-compliance with data protection regulations.

Incident Disclosure for Form 8-K

Incident Description:

Flair Airlines recently discovered unauthorized access to its web server at https://flyflair.com, attributed to the AndroxGh0st malware. This breach resulted in the exposure of sensitive customer data, including names, emails, phone numbers, and flight details. The compromised data could potentially be used for identity theft and other malicious activities. Flair Airlines promptly addressed the vulnerability and initiated measures to protect customer information and enhance cybersecurity measures.

Liability Assessment:

The company may face liabilities under GLBA and potential repercussions under SOX, as the incident could impact financial reporting accuracy and shareholder trust. Flair Airlines is committed to ensuring the security and privacy of its customers' data and will continue to cooperate with regulatory authorities to mitigate risks and protect stakeholders' interests.

Conclusion:

It is imperative for Flair Airlines to adhere to federal regulations, prioritize cybersecurity, and maintain transparency in disclosing incidents to stakeholders. The company should continue to invest in robust cybersecurity measures to safeguard customer data and uphold its commitment to regulatory compliance and stakeholder trust.

Brian F. Smith