To: Management and Board of Directors

Executive Summary:

This audit report evaluates the digital identity management system implemented on the Superior Scheduling Home Page, focusing on its adherence to NIST Special Publication 800-63B guidelines. Our objective is to ensure robust security measures while maintaining user convenience.

Methodology:

Our audit methodology included:

- Reviewing the website's password policies to ensure they adhere to NIST 800-63B guidelines, including considerations for complexity, expiration, and the promotion of passphrase usage.
- Assessing the robustness of account recovery processes to prioritize compliance with NIST 800-63B standards, facilitating only legitimate user access
- Examining session management practices, including configurations related to session locking and timeout settings, to ensure they align with NIST 800-63B guidelines
- Analyzing the implementation of multi-factor authentication (MFA) mechanisms to assess adherence to NIST 800-63B recommendations regarding the diversity and resilience of verification factors.

Results:

Our comprehensive assessment revealed strong adherence to NIST 800-63B guidelines across various aspects of the digital identity management system on the Superior Scheduling Home Page. Notably, our review of password policies highlighted a strict enforcement of complexity requirements and the elimination of expiration policies, demonstrating a commitment to robust security practices. Furthermore, the promotion of passphrase usage was found to enhance user experience without compromising security. Similarly, our analysis of MFA implementation identified a well-rounded approach, with diverse verification factors aligning seamlessly with NIST 800-63B recommendations to bolster account security. Overall, our findings indicate that the digital identity management system meets the requirements set forth by NIST 800-63B guidelines, providing both security and user-friendliness.

Risk Analysis:

From a quantitative standpoint, the risk associated with the digital identity management system appears relatively low due to the implementation of strong password policies, MFA mechanisms, and efficient session management practices. These measures collectively reduce the likelihood of unauthorized access and mitigate potential financial losses resulting from security breaches.

Qualitatively, however, it is important to acknowledge inherent risks that persist despite the system's robustness. Factors such as emerging attack routes, human error, and unforeseen vulnerabilities pose challenges. Therefore, while our quantitative assessment points to a

low risk level, qualitative nuances demonstrate the need for sustained risk management efforts and heightened security.

Recommendations:

To further strengthen the digital identity management system, we propose these strategic actions:

1. Implement a regimen of ongoing monitoring and updates to effectively address the dynamic landscape of cybersecurity threats.
2. Prioritize comprehensive security awareness training for both employees and users to foster a culture of vigilance and adherence to best practices (NIST)

By implementing these recommendations, Superior Scheduling can fortify its security posture, uphold user trust, and ensure customer satisfaction.

To: Management and Board of Directors

Executive Summary:

This audit assesses the Information and Technology (I&T) management practices at Ashley Madison, particularly focusing on the security vulnerabilities highlighted in Ars Technica's article. Our examination

reveals deficiencies in implementing COBIT governance principles, notably the use of MD5 hashes for user authentication.

Methodology:

Our audit methodology included:

- Examining the organization's adherence to COBIT governance principles, particularly regarding user authentication and data security.
- Assessing risk management strategies, including identification of vulnerabilities and implementation of mitigating controls.

Results:

Ashley Madison's I&T management practices do not meet level 4 capability standards in defined IT processes and risk management. The use of MD5 hashes for password storage poses significant security vulnerabilities, indicating a lack of adherence to industry standards.

Risk Analysis:

Qualitatively, the use of MD5 hashes poses severe risks to data confidentiality and integrity, potentially leading to reputational damage and legal consequences. Quantitatively, the estimated financial impact of a breach underscores the urgency of addressing this security vulnerability.

Recommendations:

To address deficiencies, we recommend upgrading cryptographic algorithms, enhancing the IT governance framework, implementing a formal risk management framework, and investing in cybersecurity awareness training for employees. These actions are crucial to fortify password security and mitigate the risk of data breaches.