lumin
DIGITAL

WHITE PAPER

Digital banking security

Introduction

Lumin Digital takes security and confidentiality extremely seriously. Our dedicated Enterprise Risk Management department comprises specialized risk management, security operations, and security engineering teams. Led by the Chief Risk Officer (CRO), who has a background in cybersecurity technical leadership in large fintech platforms, these teams design and implement the information security program throughout all areas of our business. Security is represented at the highest levels of the company, with our CRO reporting directly to our CEO and meeting with our senior leadership team weekly and our Board of Directors periodically to discuss issues and initiatives.

We share this information with interested parties to transparently communicate how we value and protect sensitive data through a comprehensive information security program. This document is not confidential, but it is protected by copyright. We have made our best effort to ensure all information herein is accurate as of the date of publication, June 28, 2024. The information contained in this whitepaper applies only to Lumin Digital and not any other product or service offering unless otherwise noted.

Program governance

As an independent company, our Board of Directors authorizes and provides governance oversight of Lumin Digital's information security program.

Lumin Digital has directed our Chief Risk Officer to implement an information security management system, including enterprise risk management, cybersecurity, third-party vendor management, and compliance monitoring with applicable laws, rules, and regulations. The CRO regularly reports to program stakeholders on the efficacy of controls and the overall status of the information security program.

Lumin Digital and its information security management system are subject to independent audits commissioned by company management and, separately, independent audits authorized by the Board's Audit Committee and designees. The company undergoes an annual SOC 2 Type II audit, network penetration tests, and application security testing, all performed by outside experts, to provide independent assurance that the company's controls are working as designed. The Audit Committee and its designated partners.

Policies and procedures

Information security policies, procedures, and standards are approved by leadership and made available to all Lumin Digital employees. The company strives to operate a transparent program and also makes many policies available for prospective and current clients to inspect on the company's trust portal at lumindigital.com

Lumin Digital continually reinforces policy awareness through regular attestations and provides education through its security awareness program and computer-based training. Lumin Digital defines a formal methodology for implementing its information security management system and has approved policies and procedures that include but are not limited to:

1. Acceptable Use Policy
2. Access Control Policy
3. Agreement Authorization Policy
4. Approved Locations for Storing Data
5. Asset Management Policy
6. Audit Logging Policy

7. Authentication and Password Policy
8. Backup Policy
9. Business Continuity Plan
10. Card Account Data Display Standards
11. Change Management Policy
12. Code of Ethics
13. Collaboration Recording Policy
14. Compliance Program Management Policy
15. Customer Authentication Policy
16. Data Classification Policy
17. Encryption Policy
18. Enterprise Certificate Authority Policy
19. Information Security Program
20. Logging Configuration Standards for Cloud Environment Hosts
21. Mobile Device Management Policy
22. Network Firewall Configuration Standards
23. Network Firewall Policy
24. Patching Policy
25. Physical Security Policy
26. Regulatory Change Management Policy
27. Risk Management Policy
28. Secure Application Design and Coding Standards
29. Security Incident Management Policy
30. Security Incident Reporting Policy
31. Security Incident Reporting Procedure
32. Security Incident Response Plan
33. Sensitive Data Retention Policy
34. Sensitive Data Retention Standard
35. Sensitive Data Transmission Standard
36. Sensitive Media Management Policy
37. Threat Intelligence Sharing Policy
38. Vendor Management Program
39. Vulnerability Management Program

Securing our workforce

Each member of the Lumin Digital team is critical to providing security for our products, services, clients, and end users. We are committed to recruiting, selecting, and hiring the right people who are not only security-compliant but are security-conscious and improve our overall security posture.

Background checks

Lumin Digital employs and contracts individuals authorized to work in the United States and Canada. Only US-based employees are eligible to work in roles with access to, or that can affect the security of sensitive data, and the company limits access to sensitive data to devices operating within the U.S. Lumin Digital leverages a dedicated Human Resources team to vet candidates thoroughly. We perform extensive pre-employment screening, including criminal background checks, employment, and education verification.

Security awareness and training

Upon hire and at least annually, Lumin Digital provides user awareness training for information security. Moreover, specific company policies and procedures are provided to all new hires, and role-specific, in-depth training is provided for sensitive roles, such as software developers and system administrators. Ongoing awareness is promulgated through regular updates through e-mail, internal chat, and intranet systems to provide current and relevant information to financial services, digital banking, and general use cases.

Code of ethics

Lumin Digital's code of ethics reflects our leadership's commitment to doing the right thing for our clients, end-users, and employees. Our code requires employees to be aware of and report conflicts of interest and requires managers to record, investigate, act on, and escalate all reports as necessary. We strictly prohibit questionable and unfair business practices, including self-dealing.

Product security

Our Enterprise Resource Management (ERM) team maintain a formal digital banking threat model and security risk register, and the team uses these to inform and track its collaborative work with the Product Management team to ensure features are secure by design. Similarly, our Security Operations team is tightly integrated with the Application Development teams to ensure secure designs and coding practices are developed, provided, and used as part of a Secure Software Development Life Cycle (SSDLC).

Secure by design

The CRO and Chief Product Officer coordinate to continually update a formal Product Development Lifecycle that incorporates security assessments early into the design phase of feature development. Separately, the CRO and the Chief Technology Officer measure long-term program development against the Building Security In Maturity Model (BSIMM) for software development. Collaborative efforts to ensure security is built into the product throughout the lifecycle include:

- Representation by Security throughout the Agile Scrum process
- Collaborative development of product user stories as part of the Product Development Life Cycle with Security participation
- Documented cryptographic and other security standards provided as an informative reference to all software developers
- Architectural reviews of software designs before development begins
- Formal peer and security code review procedures
- Automated security quality assessments
- Dependency vulnerability scanning

Lumin Digital rigorously tests its application source code's security and operating environments. Our layered security testing strategies include static, dynamic, and interactive testing performed by third-party companies and contractors for additional security verification and assurance.

Cryptography

Lumin Digital's banking solutions utilize Transport Layer Security (TLS) 1.2 or better encryption protocols and support strong implementation characteristics, including forward-secrecy ciphers, certificate transparency, and out-of-band protocol improvements like HSTS and DNSSEC, to ensure secure communications between end users and digital banking. Lumin Digital encrypts communications with each institution's third-party providers over encrypted private circuits, virtual private networks (VPNs), or TLS. We protect cryptographic keys using comprehensive, PCI-compliant key lifecycle management policies and procedures, which include leveraging cryptographically secure containers (or critical management systems) to protect access to encryption keys.

Account security

Lumin Digital provides multiple layers of risk-based authentication to protect digital banking users from threats to information security and confidentiality. Passwords are salted and cryptographically hashed using industry-standard password-based key derivation functions with thousands of iterations of HMAC digest algorithms. They cannot be decrypted, logged, or stored reversibly.

Digital banking users must verify a device for two-factor authentication (2FA) and are step-up challenged using a risk-based authentication strategy that uses user behavior, device fingerprinting, and multiple threat intelligence sources. Our products and corporate users have options for robust, phishing-resistant 2FA mechanisms such as Webauthn and Passkeys that protect individuals from social engineering attacks. When we observe unusual activity or other high-risk indicators, users may be either challenged for step-up 2FA authentication or outright rejected from accessing an account.

Hosting security

The security of our infrastructure, including all systems and networks, is critical. Lumin Digital has developed internal technology and configuration standards to consistently implement industry best practices for hardening environments and securing data. We align our hosted controls to the Amazon Web Service (AWS) Well-Architected Framework, the Center for Internet Security's Critical Security Controls, and the Cloud Security Alliance's Cloud Controls Matrix. Among many other frameworks, our technical and physical controls are additionally prescribed by and informed by the NIST Cyber Security Framework, the PCI Data Security Standard, and guidance from the FFIEC and other Prudential Regulators.

Lumin Digital leverages AWS's secure public cloud services within the continental United States. No client data or cryptographic keys are stored on infrastructure outside US regions. As part of a shared responsibility model, AWS provides many benefits and tools to protect sensitive data, and we use all available tools in a manner consistent with security best practices. In summary, our approach is:

1. **Asset management processes** to provision resources to ensure every system and all data is accounted for with an owner and is protected with relevant, layered security controls.
2. **Doing the basics very well** prioritizes straightforward but highly effective controls like continuous vulnerability monitoring and management, real-time patch management, and anti-malware endpoint protections. These controls receive significant ongoing attention and focus on identifying and mitigating new risks quickly.
3. **Single-tenant isolation** between environments and clients separates control and data planes across multiple accounts and virtual private clouds to separate data, network traffic, and access.

4. **Segregation of duties** between users to restrict the scope of authority of each user and provide dual authorization and management oversight of access and change.
5. **Security through automation** reduces the opportunity for errors and omissions in securely and consistently provisioning hardened environments.
6. **Layered controls** provide overlapping defense-in-depth controls for each risk.
7. **Best-in-class controls** are identified and deployed. Cloud providers make many cloud security controls available, and Lumin Digital identifies and deploys additional, comprehensive solutions that best fit digital banking threat models.
8. **Logging and continuous monitoring** enable the close monitoring of real-time dashboards and key security indicators using business intelligence and data analytics tools. We retain security logs according to formal data retention policies that align with compliance requirements and industry best practices.
9. **Continuous integration of threat intelligence feeds** means threat indicators from FS-ISAC, FBI InfraGard, and other open-source and commercial sources enrich our detection and prevention capabilities in our hosted environment.
10. **Industry engagement** allows us to assess changes in the digital banking threat environment and security tools and techniques. Our ongoing participation results in a hardened infrastructure that is not static but continuously improving to address evolving threats.

Internet threat protections

Lumin Digital uses multiple network points of presence across the continental United States to detect, prevent, and mitigate the effects of distributed denial-of-service (DDoS) attacks, including advanced web application firewalls (WAFs) and botnet shields.

Similarly, Lumin Digital strictly controls and monitors egress network activity to protect against data loss and exfiltration from the digital banking environment. We utilize stringent deny-by-default access control lists to allow network activity and monitor traffic against threat intelligence feeds for a continuously evolving view of our systems.

Physical security

Data center security

Lumin Digital leverages AWS data centers within the continental United States for all production and non-production environments. AWS follows industry best practices and complies with many regulatory and industry standards.

For more information about AWS data center physical security provisions, please visit: https://aws.amazon.com/security/

Office location security

Our office locations have multiple deterrent, detective, and preventive security controls, which include 24 x 7 security guards patrolling our office buildings, employee and visitor badges with visitor sign-in and management processes, video monitoring and recording, proximity card electronic door access locks, and specialized walls and barriers that protect sensitive equipment.

Incident management

Lumin Digital has formal and tested security incident response policies, procedures, and plans, which are communicated to and trained by stakeholders who have a role in incident response. Our plans include exhaustive checklists for various incident types, including threats to physical security and pandemics. Lumin also takes a progressive stance in making it clear how external agents can report security issues and is responsive to collaborate with security researchers to confirm and resolve issues.

Business continuity and disaster recovery

High availability

Lumin Digital utilizes AWS best practices in architecting and deploying fault-tolerant designs designed to seamlessly address intermittent component or whole availability zone interruptions. By utilizing high-availability features built into AWS services and multiple availability zones, each of which is in distinct regional data centers, for each layer of our solution, our hosted digital banking platform is resilient to whole-datacenter failure without requiring a disaster recovery plan response.

Disaster recovery

By leveraging automation for all aspects of its digital banking solution software and infrastructure, Lumin Digital readily has options for resuming services in different AWS geographical regions. Lumin Digital's Operations teams maintain disaster recovery plans and test them at least annually, updating them as necessary. Disaster recovery plans provide for the resumption of services for unusual and rare interruptions or disasters that affect multiple data centers within one geographic region.

Business continuity

Lumin Digital has and regularly updates a formal business continuity plan to strategize recovery controls for various business interruption scenarios. Comprehensive plan testing is routinely conducted at leadership and operational levels, using walkthrough scenarios and simulation-based testing.

Third-party vendor security

Lumin Digital has a formal vendor management policy and vetting procedure, including due diligence reviews of applicable security controls and prospective vendor risk assessments. We have formal data security requirements we impose on vendors to allow our clients to manage fourth-party risk through assurances we obtain from our service providers related to the security, confidentiality, and management of sensitive data.

Summary

Lumin Digital operates a comprehensive information security management system. We invest significantly in people, processes, and tools with appropriate oversight and business integration to ensure we can effectively fulfill our security and compliance obligations. Specialists in cybersecurity with experience protecting large-scale, cloud-based financial technology solutions lead our information security program. We supplement our in-house expertise with industry partners and external information sources to quickly adapt and continuously improve our security program and posture.

Lumin Digital combines our strong information security program with a commitment to transparency to give our clients the confidence to trust us to provide a best-in-class digital banking solution.

If you have additional questions or require further details, please contact our Security team through our Sales team at contact@lumindigital.com.

lumindigital.com | 3001 Bishop Drive, Suite 110 | San Ramon, CA 94583 | 925.359.9560

240820