lumin DIGITAL

WHITE PAPER

Digital banking security

Introduction

Lumin Digital takes security and confidentiality extremely seriously. Our dedicated Risk department comprises specialized enterprise risk management professionals, security operations and engineering teams, and a privacy engineering discipline. Led by Dr. Sean McElroy, Chief Risk Officer, who has a proven track record of building and securing large digital banking and fintech platforms, our teams design and implement the information security program to protect data for nearly 100 clients and over 8 million consumers across our offerings. Information security is represented at the highest levels of the company, with our CRO reporting directly to our CEO and meeting weekly with our executive leadership team and regularly with our Board of Directors to discuss emerging threats, risks, and initiatives to address them.

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, July 31, 2026. The information contained in this whitepaper applies solely to Lumin Digital's digital banking service 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 testing, and application security testing, all performed by external experts, to provide independent assurance that the company's controls are functioning as designed. Separately, the Audit Committee and its designated partners conduct their own risk assessments and audits of the company's operations and this program. These independent assessments culminate in multiple reports on our compliance and program health, including those related to adhering to the PCI Data Security Standard.

Policies and procedures

Information security policies, procedures, and standards are approved by leadership and made available to Lumin Digital employees. The company strives to operate a transparent program and also makes relevant policies available for prospective and current clients to inspect on the company's trust portal at https://trust.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. Approved Locations for Storing Data

4. Asset Management Policy
5. Audit Logging Policy
6. Authentication and Password Policy
7. Backup Policy
8. Business Continuity Plan
9. Card Account Data Display Standards
10. Change Management Policy
11. Code of Ethics
12. Collaboration Recording Policy
13. Customer Authentication Policy
14. Data Classification Policy
15. Data Classification and Protection Standards
16. Encryption Policy
17. Endpoint Security Policy
18. Enterprise Certificate Authority Policy
19. Generative AI Acceptable Use Policy
20. Government Information Request and Disclosure Policy
21. Information Security Program
22. Logging Configuration Standards for Cloud Environment Hosts
23. Mobile Device Management Policy
24. Network Firewall Policy
25. Patching Policy
26. Physical Security 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 Response Plan
32. Sensitive Data Retention Policy
33. Sensitive Data Retention Standard
34. Sensitive Data Transmission Standard
35. Sensitive Media Management Policy
36. Threat Intelligence Sharing Policy
37. Vendor Management Program
38. Vulnerability Management Program

Securing our workforce

Each member of the Lumin Digital team is critical to ensuring the security of 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 also 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 U.S.-based employees are eligible to work in roles that have access to, or the ability to affect, the security of sensitive data. Furthermore, the company limits access to sensitive data to devices operating within the U.S. Lumin Digital leverages a dedicated Human Resources team to thoroughly vet candidates. 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 maintained through regular updates via e-mail, internal chat, and intranet systems to provide current, relevant information on 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 Risk teams maintain a formal digital banking threat model and security risk register, which they use to inform and track their 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 that secure design and coding practices are developed, delivered, and used throughout the secure Software Development Life Cycle.

Secure by design

The CRO and Chief Product and Technology Officer oversee updates to a formal, documented Product Development Lifecycle that incorporates security assessments early into the design phase of feature development. The Application Security team within Risk measures 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 the security of its application source code and operating environments. Our layered security testing strategies include static, dynamic, and interactive testing conducted by third-party companies and contractors to provide additional security verification and assurance.

Cryptography

Lumin Digital's banking solutions use Transport Layer Security (TLS) 1.3 and support strong implementation characteristics, including forward-secrecy ciphers, certificate transparency, and out-of-band protocol improvements such as HSTS and DNSSEC, to ensure secure communication between end users and digital banking services. 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 through comprehensive, PCI-compliant key lifecycle management policies and procedures, including the use of cryptographically secure containers (or key management systems) to control 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-leading password-based key derivation functions (including Argon2id). They cannot be decrypted, logged, or stored in a reversible manner.

Digital banking users must verify a device for two-factor authentication (2FA) and are step-up-challenged using a risk-based authentication strategy that leverages user behavior, device fingerprinting, and multiple threat intelligence sources. Our products and corporate users offer 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 prompted to step up to 2FA or outright denied access to an account.

As part of our service offering, Lumin Digital operates a Security Operations Center that monitors network and application security activity. The SOC team leverages private ISAC/ISAO threat intelligence, machine-learning-driven fraud detection tools, and enterprise-grade bot management services to tune automated cybersecurity defenses and step in for manual mitigations as needed to protect our clients and their consumers from volumetric and automated threats.

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 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 prescribed and informed by the NIST Cybersecurity Framework, the PCI Data Security Standard, and guidance from the FFIEC and other Prudential Regulators.

Lumin Digital leverages Amazon Web Services' secure public cloud services within the continental United States. No client data or cryptographic keys are stored on infrastructure outside U.S. 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** for provisioning resources ensure that every system and all data are accounted for by an owner and protected by relevant, layered security controls.

2. **Doing the basics very well** prioritizes straightforward yet highly effective controls such as continuous vulnerability monitoring and management, real-time patch management, and anti-malware endpoint protection. These controls receive

significant ongoing attention and focus on quickly identifying and mitigating new risks.

3. **Single-tenant isolation** between environments and clients separates the control and data planes across multiple accounts and virtual private clouds, isolating 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 opportunities for errors and omissions in the secure and consistent provisioning of 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 offer many cloud security controls and services, and Lumin Digital identifies and deploys additional, comprehensive solutions that best address evolving digital banking threat models.
8. **Logging and continuous monitoring** enable real-time visibility into dashboards and key security indicators through business intelligence and data analytics tools. We retain security logs in accordance with formal data retention policies that align with compliance requirements and industry best practices.
9. **Continuous integration of threat intelligence feeds** means threat indicators from commercial, private, and other open-source 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 to monitor traffic against threat intelligence feeds, providing 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, including 24/7 security guards patrolling our office buildings; employee and visitor badges with sign-in processes; video monitoring and recording; proximity-card-controlled electronic door access locks; and specialized walls and barriers that protect sensitive equipment.

Incident management

Lumin Digital has formal, tested security incident response policies, procedures, and plans, which are communicated to and training is provided to 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 by making it clear how external agents can report security issues, and is responsive to collaboration with security researchers to confirm and resolve them quickly and amicably.

Business continuity and disaster recovery

High availability

Lumin Digital utilizes AWS best practices to architect and deploy fault-tolerant designs that seamlessly address intermittent component or entire availability zone interruptions. By utilizing high-availability features built into AWS services and multiple availability zones, each in distinct regional data centers for each layer of our solution, our hosted digital banking platform is resilient to whole-data-center failures within a region. As evidenced by our SOC 2 Type II reporting, our Operations teams regularly test this resiliency through seamless cutover testing, with oversight by our Risk teams, who review the design and effectiveness of availability controls.

Disaster recovery

By leveraging automation across all aspects of its digital banking software and infrastructure, Lumin Digital has options to resume services in different AWS geographic 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 during unusual or rare interruptions or disasters that affect multiple data centers within a single geographic region.

Business continuity

Lumin Digital 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 ongoing due diligence reviews of applicable security controls and risk assessments of prospective vendors. We have formal data security requirements that we impose on vendors, enabling our clients to manage third-party risk through assurances we obtain from our service providers regarding the security, confidentiality, and management of sensitive data.

AI governance

Artificial intelligence, including machine learning and generative large language models, offers substantial benefits in delivering digital banking services, but requires deliberate governance to preserve the security, confidentiality, and integrity of client and consumer data. Lumin Digital's Risk department leads AI governance jointly with our Legal department, across both consumer-facing product features and internal corporate use.

AI use cases are subject to the same risk assessment, secure development, and third-party due diligence considerations as the rest of our platform. Formal policies, including our Generative AI Acceptable Use Policy and enterprise LLM integration

guidelines, govern them. We do not use client or consumer data to train third-party or publicly available models. Any use of data for in-house models (such as to detect security or fraud threats) is consistent with our data classification standards and privacy controls.

Where we offer AI-enabled product features, we enforce data protection standards through contractual agreements with our service providers. Where AI informs decisions affecting consumers, we maintain appropriate documentation, human oversight, and evaluate models for reliability and fairness. The NIST AI Risk Management Framework informs our approach.

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 confidence in our ability to deliver a trustworthy, compounding growth platform.

For additional questions or further details, prospective clients and partners can reach our security leaders through our Sales team via contact@lumindigital.com or find further due diligence information on demand at https://trust.lumindigital.com/. Security researchers can find direct contact information through the standard `security.txt` mechanism.

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

081926