Walking the Walk to Protect Customer Information

Major consumer financial services provider affirms SparkPost's adherence to security and business controls

> "SparkPost demonstrates a mature security culture with the utmost commitment to good security and business controls. SparkPost's industry-leading email delivery expertise is backed by a sound and secure technical and business operation."

OVERVIEW

When a major consumer financial services provider embarked on an ambitious program to consolidate its diverse customer messaging programs under a single entity in the company, they quickly realized that SparkPost's email infrastructure was the clear choice for delivering high performance and maximizing customer engagement. But as a business entrusted with consumers' most sensitive financial data, the bank needed to ensure that their technology provider did not make compromises that might jeopardize the business' well-earned trust.

This financial services firm needed to have confidence that:

→ Their service provider's technology platform incorporated all practical **security features and was hardened to external threats**.

→ The application architecture enforced **stringent policies and procedures to protect customer information**, and

→ The partner **followed best practices for operational control** of its processes and systems.

With these iron-clad imperatives defined, the bank met with SparkPost's engineering, operations, professional services, product management, and executive teams to carefully examine SparkPost's technology implementation and business practices. The audit confirmed that SparkPost demonstrates the utmost commitment to mature security and operational controls. While many of the specific evaluation criteria of this bank's security assessment remain confidential, SparkPost's commitment to good security practices is no secret. This fidelity permeates our technical architecture design, our treatment of customer information, and our operational practices.

SPARKPOST IS ARCHITECTED FOR SECURITY

SparkPost was designed from the start as a robust technology platform, and good security practices are fundamental to the platform's architecture. Key features and attributes include:

- End-to-end encryption with transport-layer security across all services, to prevent interception of data communications.

- Operational controls such as IP address restrictions, unique API keys, and multi-factor authentication, to ensure only authorized access to systems.

- Active risk management including exploit vulnerability scans, penetration testing, and access monitoring, to proactively defend against threats.

- Infrastructure redundancy to provide resilience and continuity of service against distributed denial of service (DDoS) attacks.

- Configuration controls that include establishing baselines and auditing each deployment for consistency.

- Integral security design considerations and regular code reviews, to ensure security at every level.

- Leverage of certified Amazon Web Services cloud infrastructure. Certifications include ISO 27001, SOC, the PCI Data Security Standard, FedRAMP, and others.

SPARKPOST PROTECTS CUSTOMER PRIVACY

SparkPost is in the business of delivering transactional and marketing messages for our customers, not aggregating consumer records for monetization. However, even the minimal customer data we process for message delivery — email address and resulting delivery and user engagement metrics — must be protected from inappropriate access. The measures we take to protect customer information include:

- Personally-identifiable information (PII) is limited to name, email address, and IP address of user interactions with email messages.

- PII data has limited shelf life in our system. After ten days, only anonymous, aggregate deliverability and engagement metrics are kept.

- Customer databases are fully separated in SparkPost Elite and use encrypted data storage.

- Database queries limited by IP address, API key, and other restrictions.

SPARKPOST ENSURES BUSINESS CONTROL

Good security means more than hardened technology; it also requires sound business processes that support technical controls. At SparkPost, that business control underlies how we implement technical infrastructure. Key operational considerations include:

- Defined information security practices, backed by a culture of security and an accountable Chief Information Security Officer (CISO).

- Change management controls and quality assurance practices that minimize the likelihood of disruption, unauthorized alterations, and errors.

- Compliance with legal and regulatory requirements and contractual obligations.

- Risk management framework, crisis response procedures, and business continuity plans.

- Sound operational management of IT systems, continuous monitoring of all production infrastructure, and timely response to issues.

- Physical site control with well-defined access procedures.

NO COMPROMISES

When this financial services provider examined SparkPost's security practices, it confirmed what we already knew: SparkPost demonstrates a mature security culture with the utmost commitment to good security and business controls. The bank's audit gave the company confidence that SparkPost's industry-leading email delivery expertise is backed by a sound and secure technical and business operation. The responsibility and trust for protecting our customers' business information underlies every aspect of our technical architecture design, our treatment of customer data, and our operational practices.

→ **Learn More About SparkPost Today.**
Follow us on Twitter **@sparkpost** or go to **sparkpost.com**.

About SparkPost

SparkPost is the cloud solution from the world's number one email infrastructure provider, whose customers — including Pinterest, Twitter, CareerBuilder, LinkedIn, Groupon, Salesforce, Marketo, Zillow, and Comcast — send over 3 trillion messages a year, over 25% of the world's legitimate email. Our service outperforms every other cloud or on-premises alternative, and these companies choose us to provide the deliverability, speed and insight they need to drive customer engagement for their business.