Security Overview for Financial Institutions

Vendor Security Assessment Documentation

Version: 1.0 **Date:** February 2026

No Member PII

Anonymous service. Members use ScamZero without creating accounts or sharing personal information.

12-Hour Auto-Delete

All user-submitted content is automatically purged within 12 hours. We can't lose what we don't keep.

SOC 2 Vendors

Built entirely on enterprise-grade infrastructure from Cloudflare, Google, and SendGrid.

Contents

1. Service Description

ScamZero provides a white-labeled **Scam Safety Center** that credit unions deploy for their members. The platform enables members to:

- **Forward suspicious emails** for AI-powered risk analysis
- **Upload screenshots** of text messages or DMs to check for scam indicators
- **Access educational content** about current scam threats
- **Get recovery guidance** if they've fallen victim to a scam

> ✓ Key Design Principle
>
> ScamZero is an **anonymous, educational service**. Members visit the portal like any public website - no login required, no accounts created, no personal information collected. This architecture eliminates entire categories of security risk.

What ScamZero Is NOT

- ✕ A fraud detection system integrated with core banking
- ✕ A transaction monitoring service
- ✕ A system that accesses member accounts or financial data
- ✕ A service that makes definitive "scam" or "safe" determinations

2. Data Handling

Data We Collect

Data Type	Source	Retention	Purpose
Organization profile	CU admin signup	Until account deletion	Portal customization
Admin email/name	CU admin signup	Until account deletion	Authentication, alerts
Forwarded emails	Member submissions	**12 hours (auto-deleted)**	Scam analysis
Uploaded screenshots	Member submissions	**12 hours (auto-deleted)**	Scam analysis
Analysis results	System-generated	12 hours (shareable link)	Member review
AI chat conversations	Member submissions	**30 days (Zapier)**	Scam questions

Data We Do NOT Collect

- ✕ Member names
- ✕ Social Security numbers
- ✕ Account numbers
- ✕ Financial data
- ✕ Member passwords
- ✕ Payment card data
- ✕ Biometric data
- ✕ Location data

ℹ️ **Data Residency**

All data is processed and stored in the United States via Cloudflare's infrastructure. No data is transferred to or stored outside US jurisdiction.

3. Security Controls

Encryption

Layer	Standard	Implementation
Data in Transit	TLS 1.3	Enforced HTTPS on all connections
Data at Rest	AES-256	Cloudflare D1 and R2 encryption
API Communications	TLS 1.3	Encrypted end-to-end with vendors

Application Security

- ✓ **Input validation:** All user inputs sanitized against injection attacks
- ✓ **AI prompt injection protection:** Content filtered for manipulation attempts
- ✓ **XSS prevention:** HTML encoding on all outputs
- ✓ **CSRF protection:** Cloudflare Turnstile on all forms
- ✓ **Rate limiting:** 30 requests/minute per IP
- ✓ **CORS:** Restricted to allowed origins only

Authentication (Admin Portal Only)

Only credit union administrators access the admin portal. Members use the service anonymously.

- ✓ **Passwordless login:** Magic link via email (no passwords to steal)
- ✓ **JWT tokens:** HMAC-SHA256 signed, time-limited sessions
- ✓ **Secure cookies:** HTTP-only, Secure, SameSite flags

ℹ️ Why No SSO or MFA?

SSO: Not applicable. Members don't log in - the service is anonymous. Admin accounts are limited to a few CU staff members who authenticate via magic link.

MFA: Magic link authentication provides similar security to MFA - access requires control of the registered email account. Traditional MFA is on our roadmap for admin accounts.

4. Infrastructure

✓ No Self-Hosted Servers

ScamZero runs entirely on Cloudflare's serverless platform. This eliminates server management, patching, and the associated security risks of managing our own infrastructure.

Cloudflare Services Used

Service	Purpose	Security Benefit
Workers	Application logic	Isolated execution, auto-scaling
Pages	Static site hosting	Global CDN, DDoS protection
D1	Database	Encrypted at rest, automated backups
R2	Object storage	Encrypted, 11 9's durability
WAF	Web Application Firewall	Blocks common attack patterns
Turnstile	CAPTCHA	Bot protection without friction

Cloudflare Certifications

Cloudflare maintains the following certifications:

SOC 2 TYPE II ISO 27001 PCI DSS FEDRAMP MODERATE

5. Third-Party Vendors

Vendor	Service	Data Access	Certifications
Cloudflare	Hosting, CDN, Database, WAF	All application data	SOC 2, ISO 27001, PCI DSS
Google Cloud	Gemini AI API	Email/screenshot content (transient, not retained)	SOC 2, ISO 27001, FedRAMP
Google	Safe Browsing API	URLs only (hashed)	N/A (public API)
SendGrid (Twilio)	Email delivery	Admin emails, notifications	SOC 2, ISO 27001
Stripe	Payment processing	Billing (not stored by ScamZero)	PCI DSS Level 1
Zapier	AI chatbot service	Chat conversations (30-day retention)	SOC 2

ℹ️ **AI Data Processing**

Email and screenshot content sent to Google Gemini for analysis is processed in real-time and not retained by Google. Google's Gemini API operates under their standard Cloud data processing terms, which prohibit using customer data for model training.

6. Incident Response

Detection

- ✓ Real-time logging via Cloudflare Analytics Engine
- ✓ Rate limiting triggers monitored
- ✓ API errors and anomalies tracked
- ✓ Security event logging

Response Commitment

Severity	Description	Response Time
Critical	Active breach, data exposure	Immediate
High	Potential breach, significant vulnerability	4 hours
Medium	Minor vulnerability, isolated issue	24 hours

✓ Breach Notification

In the event of a confirmed data breach affecting customer data, ScamZero will notify affected organizations within **72 hours** of discovery, consistent with NCUA guidance and industry best practices.

7. Compliance Alignment

Requirement	Status	Notes
GLBA	NOT APPLICABLE	ScamZero does not collect member Nonpublic Personal Information (NPI). See separate GLBA Statement.
NCUA Vendor Guidance	ADDRESSED	This document provides information for NCUA third-party risk management requirements.
Nacha 2026	SUPPORTIVE	ScamZero helps demonstrate "reasonable procedures" for member fraud education. See Nacha 2026 Compliance Brief.
SOC 2 Type II	VIA VENDORS	ScamZero leverages SOC 2 certified infrastructure (Cloudflare, Google, SendGrid). ScamZero's own SOC 2 certification is on our roadmap.
WCAG 2.1 AA	COMPLIANT	VPAT documentation available upon request.

8. Contact Information

All inquiries	support@scamzero.com
Website	scamzero.com
Trust Center	scamzero.com/trust-center