# Security Overview

Vendor Security Assessment for Public Agencies, Universities, and Nonprofits

**Version:** 1.1 **Date:** August 2026

### No Resident PII

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

### 24-Hour Auto-Delete

Submitted content is never written to storage on the scam-check path. The assessment it produces is deleted the moment the person opens it, and expires automatically if it is never opened. One exception: an email forwarded from an address that has not yet been confirmed is held, unanalyzed, for up to 24 hours so the confirmation link keeps working, then deleted. 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 police departments, cities and counties, universities, and nonprofits deploy for the people they serve. The platform enables residents 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 any account, roster, or record the organization holds
- ✕ A service that makes definitive "scam" or "safe" determinations

## 2. Data Handling

### Data We Collect

| Data Type | Source | Retention | Purpose |
|---|---|---|---|
| Organization profile | Organization admin signup | Until account deletion | Portal customization |
| Admin email/name | Organization admin signup | Until account deletion | Authentication, alerts |
| Forwarded emails | Resident submissions | **Deleted on first view; 1 hour max; 15 min if no link requested** | Scam analysis |
| Uploaded screenshots | Resident submissions | **Not stored — analyzed in memory** | Scam analysis |
| Analysis results | System-generated | Deleted on first view; expires automatically if never opened | Member review |

### Data We Do NOT Collect

- ✕ Resident names
- ✕ Social Security numbers
- ✕ Account numbers
- ✕ Financial data
- ✕ Resident 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. Application data is stored in the United States. Cloudflare's global edge network may process a request at the data center nearest the visitor; contact us to discuss data-residency options.

## 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
- ✓ **Bot and abuse mitigation:** Cloudflare Turnstile on public forms. Cross-site request forgery is addressed separately by SameSite cookie attributes.
- ✓ **Rate limiting:** per-endpoint hourly windows (for example 5 contact submissions and 10 situation checks per hour, per IP) plus a daily per-person check quota
- ✓ **CORS:** Restricted to allowed origins only

### Authentication (Admin Portal Only)

Only administrators the organization designates access the admin portal. Residents 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 the staff the organization designates 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 |

| Service | Purpose | Security Benefit |
|---|---|---|
| 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 |
| **Cloudflare, Inc.** | Workers AI (scam analysis) | Submitted text and screenshots, processed in memory. Never written to storage. | SOC 2, ISO 27001 |
| **Google** | Google Web Risk API | The complete submitted URL, sent in full rather than hashed | N/A (public API) |

| Vendor | Service | Data Access | Certifications |
|---|---|---|---|
| **SendGrid (Twilio)** | Email delivery | Admin emails, notifications | SOC 2, ISO 27001 |
| **Stripe** | Payment processing | Billing (not stored by ScamZero) | PCI DSS Level 1 |

ℹ️ AI Data Processing

Email and screenshot content sent to Cloudflare Workers AI is processed in memory and never written to storage. Cloudflare's published Workers AI data policy states that it does not retain inputs or outputs and does not use them to train any model. The model itself (Gemma 4) is open-weights and runs on Cloudflare's network; no submission is sent to Google.

## 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 |

| Severity | Description | Response Time |
|---|---|---|
| **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, and ScamZero will cooperate with the organization's own notification obligations under applicable state breach-notification law.

## 7. Compliance Alignment

| Requirement | Status | Notes |
|---|---|---|
| **GLBA** | NOT APPLICABLE | ScamZero does not collect member Nonpublic Personal Information (NPI). See separate GLBA Statement. |
| **State breach-notification statutes** | ADDRESSED | This document provides the vendor information a public agency or university needs for its own third-party risk review. |
| **Nacha 2026** | SUPPORTIVE | ScamZero helps demonstrate "reasonable procedures" for member fraud education. See Nacha 2026 Compliance Brief. |

| Requirement | Status | Notes |
| --- | --- | --- |
| **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 |