VolunteerBadge

Security Posture & Data Protection Overview

How VolunteerBadge protects volunteers, organizations, and screening data

Prepared for organizations evaluating VolunteerBadge for volunteer background screening. This document describes the security and privacy controls in effect across the platform.

Questions? support@screenforgelabs.com · (239) 219-0929

VolunteerBadge — a product of ScreenForge Labs, LLC · July 2026

VolunteerBadge

Executive summary

VolunteerBadge, a product of ScreenForge Labs, LLC, is a volunteer background-screening platform operated as an FCRA-regulated consumer reporting agency. The data we handle — criminal background reports, identity documents, and the personal information of volunteers — is among the most sensitive data a nonprofit will ever entrust to a vendor. We designed the platform around that reality from day one.

Our approach rests on four principles: verified identity for every sensitive access path (including a mandatory biometric identity check before any API access), defense in depth (every control is enforced server-side, at multiple layers), least exposure (data is encrypted, masked, and access-scoped so information appears only where it is genuinely needed), and human accountability (records are reviewed by trained people, and every privileged administrative action is permanently logged).

We take data privacy and security seriously so that volunteers and nonprofit leaders are fully protected. This document details the specific controls in effect. For questions or a deeper review, contact support@screenforgelabs.com or (239) 219-0929.

What's inside

1 Regulatory & FCRA compliance

ScreenForge Labs, LLC operates VolunteerBadge as a consumer reporting agency regulated under the federal Fair Credit Reporting Act (FCRA). FCRA compliance is not a feature we bolted on — it is the workflow. Our team has completed FCRA training, and the platform enforces the law's requirements mechanically so organizations cannot accidentally skip them.

- **Consent-first screening —** no background check runs without the volunteer's standalone FCRA disclosure and signed authorization, captured in a secure, mobile-friendly flow and stored with the record. Organizations certify their permissible purpose.
- **Human review of every potential record —** reports that surface possible records are never released automatically. A trained reviewer confirms the record truly belongs to the applicant before anything reaches the organization — protecting volunteers from mistaken-identity harm.
- **Non-conviction handling —** clear reports exclude records older than seven years, arrests that did not lead to conviction, warrants, and dismissed cases, consistent with FCRA reporting standards for this screening class.
- **Built-in adverse action workflow —** if an organization considers declining a volunteer based on a report, the platform walks it through the required steps: Pre-Adverse Action Notice with a copy of the report and the CFPB "Summary of Your Rights," a waiting period of at least five business days, then the final Adverse Action Notice. Every step is logged in an exportable audit trail.
- **Dispute rights honored —** volunteers can dispute the accuracy or completeness of their report, triggering reinvestigation as required by the FCRA. Disputes are handled by people, not automation.
- **No adverse automation —** VolunteerBadge never auto-rejects a volunteer. Results are delivered to accountable humans at the organization, with education about individualized assessment built into the product.

Why this matters to your board

FCRA violations carry statutory damages and class-action exposure for the organizations that order reports — not just the screening vendor. A platform that enforces disclosure, authorization, human review, and adverse-action timing structurally reduces your organization's own legal risk.

2 Identity & access management

Two-factor authentication (2FA)

- **TOTP 2FA for every account —** any user can protect their sign-in with a 6-digit rotating code from an authenticator app (Google Authenticator, Microsoft Authenticator, Authy, 1Password, and others). Enrollment takes about two minutes with a QR code.
- **Server-side enforcement —** an account with an enrolled authenticator cannot be used with a password alone. The requirement is enforced in the authentication layer on every page load and every API route — not just at the login screen — so a stolen password opens nothing.
- **Organization-wide 2FA policy —** owners and admins can require 2FA for their entire team. Members who have not enrolled are held at the enrollment screen until they do.
- **Mandatory 2FA for platform staff —** ScreenForge Labs administrative accounts are required to use 2FA — the admin console refuses access without an enrolled authenticator. This is enforced in code, not policy documents.

Session controls

- **Idle auto sign-out —** dashboard sessions automatically sign out after inactivity (60 minutes by default, user-adjustable between 15 minutes and 4 hours — it can be tightened but never disabled). A 60-second warning lets active users continue. This protects shared and unattended computers, a common reality in nonprofit offices.
- **Administrative session time-box —** platform staff sessions expire absolutely after 12 hours, requiring a fresh password + authenticator sign-in.
- **Sign out everywhere —** any user can instantly revoke every active session on every device from Settings !’ Security — for a lost laptop or suspected compromise.
- **Login visibility —** each user sees their own recent sign-in activity (time, IP address, device) in Settings !’ Security, and sign-in events are recorded for account-security review.

Account & role controls

- **Role-based access —** organizations assign Owner, Admin, and Coordinator roles with scoped permissions; billing and organization settings are restricted to managing roles.
- **Password protections —** passwords are stored using industry-standard adaptive hashing (bcrypt) by our authentication provider and are never visible to VolunteerBadge staff. Self-service password change and email-verified reset flows are built in.
- **Volunteer sign-in without passwords —** the volunteer portal uses one-time email codes — no passwords for volunteers to reuse, leak, or forget.

3 API & integration security

VolunteerBadge offers a REST API and a hosted MCP endpoint (for AI-assistant integrations such as Claude). Because these paths can order background checks programmatically, they carry our strictest controls.

- **Biometric identity verification required —** before ANY organization can create an API key, register a webhook, or make a single API or MCP call, an owner or admin must complete identity verification: a government-issued photo ID plus a live biometric selfie match. Unverified accounts receive a hard 403 on every request. We know who is behind every API integration.
- **API keys never stored in plaintext —** keys are shown once at creation and stored only as bcrypt hashes. Keys are revocable by the organization at any time.
- **OAuth 2.0 with PKCE for MCP —** AI-assistant connections use the OAuth 2.0 authorization-code flow with PKCE; access tokens are stored SHA-256-hashed, expire after 30 days, and are revocable by the organization.
- **Per-caller rate limiting —** every API key and MCP connection is throttled (100 requests/minute), limiting the blast radius of a leaked credential.
- **Complete request logging —** every REST and MCP call — successful or failed — is logged with organization, key, endpoint, source IP, and user agent, giving us full attribution for every programmatic action.
- **Automated abuse detection —** a scanner sweeps API traffic every 15 minutes for volume spikes, invalid-key probing (credential guessing), sustained error storms, and blocked callers that keep hammering — raising alerts to our security team in minutes, not days.
- **Instant kill switch —** ScreenForge Labs administrators can suspend all API and MCP access for any organization with one action, effective immediately across every key and token, while an investigation proceeds.
- **Signed webhooks —** outbound webhook payloads are signed with a per-endpoint HMAC-SHA256 secret so receiving systems can verify authenticity and integrity.
- **AI guardrails —** the AI integration layer refuses to accept Social Security numbers in conversation, defaults to consent-first screening, and relays adverse-action guidance rather than verdicts.

4 Encryption & data protection

In transit

- **TLS everywhere —** all traffic is encrypted in transit with TLS. HTTP Strict Transport Security (HSTS) is enforced with a two-year policy including subdomains, so browsers refuse to connect insecurely.
- **SSN application-layer encryption —** Social Security numbers receive an additional layer of application-level encryption in transit with per-context derived keys — beyond TLS — during the secure screening flows where they are collected.

At rest

- **Encrypted storage —** the production database and file storage are encrypted at rest with provider-managed AES-256 on SOC 2-audited cloud infrastructure.
- **Row-level security —** PostgreSQL row-level security policies scope data access at the database layer, in addition to application-level authorization.
- **Private media storage —** identity documents, report files, and uploaded media live in private buckets, accessible only through short-lived signed URLs generated for authorized viewers.

Special handling of Social Security numbers

- **Never in URLs —** middleware strips SSN-shaped parameters from every request URL before processing, so SSNs cannot end up in logs, browser history, or analytics.
- **Never in chat or AI —** our assistant is hard-coded to refuse SSNs in conversation. SSNs are collected only inside the dedicated secure screening flows.
- **Sensitive-path log hygiene —** API paths that can carry SSNs are flagged and sanitized in the logging layer.

Documents & payments

- **Password-protected reports —** downloadable background-check report PDFs are password-protected.
- **Payments never touch our servers —** all payment processing is handled by Stripe (PCI DSS Level 1). VolunteerBadge never stores or transmits card numbers.

5 Monitoring, auditing & abuse prevention

- **Append-only admin audit log —** every privileged action by ScreenForge Labs staff — customer-account impersonation for support, organization flags and deletions, API suspensions, admin-privilege grants — is permanently recorded with who, what, target, and timestamp. Nothing in the application can edit or delete these entries. When you ask "who accessed our account and why," we can answer precisely.
- **Support impersonation is controlled and logged —** when support staff access a customer account to help, the session is visibly bannered, time-limited by the 12-hour staff session cap, and both the start and end are written to the audit log.
- **Account risk monitoring —** automated risk signals can place organizations on hold pending identity verification, and platform administrators review flagged accounts before screening continues.
- **API traffic surveillance —** the 15-minute abuse scanner (Section 3) plus a live administrative dashboard of every API caller, their volumes, error rates, IPs, and endpoints.
- **Rate limiting beyond the API —** authentication endpoints and public AI endpoints carry their own throttles to blunt brute-force and scraping attempts.
- **Hardened HTTP responses —** every response carries baseline security headers: HSTS, MIME-sniffing protection, clickjacking (framing) protection, strict referrer policy, and a locked-down browser permissions policy.
- **Public status page —** platform status is published at status.volunteerbadge.com.

6 Infrastructure & vendor security

VolunteerBadge runs on established, independently audited cloud infrastructure rather than self-managed servers — meaning physical security, network security, and platform hardening are handled by teams that specialize in exactly that, with compliance reports to show for it.

- **Application hosting —** Vercel (SOC 2 Type II audited) serves the application at the edge with managed TLS.
- **Database & authentication —** Supabase (SOC 2 Type II audited), running PostgreSQL on AWS infrastructure with encryption at rest and managed backups.
- **Payments —** Stripe — PCI DSS Level 1, the highest certification level for payment processors.
- **Identity verification —** Didit performs government-ID and biometric liveness verification; verification media is access-controlled and served only through signed URLs.
- **Email & SMS —** transactional email via Resend; SMS via Twilio, with opt-out handling and per-day usage caps.
- **Separation of duties —** production database credentials are not distributed to developer machines; schema changes are applied deliberately through reviewed migrations, and the application is deployed from a single audited code path (version-controlled, with production promotion as an explicit human action).

> **A note on honesty**
>
> We tell evaluators what we have — and what we don't. ScreenForge Labs is an early-stage company: we do not yet hold our own SOC 2 report or ISO 27001 certification, and we say so plainly. What we do have is a platform built security-first on audited infrastructure, with the specific, verifiable controls in this document. As we grow, formal certification is on our roadmap, and this document will evolve with it.

7 Volunteer privacy commitments

Volunteers are people donating their time — often to serve children, seniors, and vulnerable neighbors. Protecting their dignity and privacy is a product principle, not a legal afterthought.

- **Consent at every step —** volunteers see the FCRA disclosure, sign their own authorization, and control optional steps (identity verification media, immunization records, character references, public profiles). Optional means optional.
- **Status-only badge — never the report —** the portable VolunteerBadge a volunteer can share is a status attestation (active/expired, validity dates). Organizations viewing a badge never see the underlying report. Reports are visible only to the organization that ordered the check with permissible purpose.
- **Health records stay separate —** verified immunization records (SMART Health Cards) are cryptographically verified, volunteer-controlled, and kept entirely separate from the background-check report. They are never part of a consumer report.
- **Character references stay separate —** reference responses are relayed opinions from people the volunteer chose — clearly separated from the background check and never treated as a consumer report.
- **We never sell data —** volunteer and organization data is used to deliver the service. It is not sold, rented, or shared for advertising. Ever.
- **Data minimization —** we collect what screening and program management genuinely require, mask what we can, and volunteers can remove optional data (public profile, health card, media) at any time.
- **Deletion & correction —** organizations can delete their accounts (cascading their data), and volunteers can dispute and correct report information through the FCRA dispute process, and request corrections or removal of directory information by contacting support.

8 Reporting a concern & contact

Security is a conversation. If your team has questions this document doesn't answer — or wants to walk through any control in detail — we will get you to a direct answer quickly.

- **Responsible disclosure —** if you believe you have found a security vulnerability in VolunteerBadge, email support@screenforgelabs.com with the details. We commit to acknowledging reports promptly, investigating in good faith, and never pursuing legal action against good-faith research.
- **Security questionnaires —** we complete vendor security questionnaires for evaluating organizations — send yours to the address below.
- **Trust Center —** deeper coverage detail about our screening sources is available at volunteerbadge.com/trust, with the most detailed information available under NDA with identity verification.

VolunteerBadge

VolunteerBadge is a product of ScreenForge Labs, LLC, an FCRA-regulated consumer reporting agency.

support@screenforgelabs.com · (239) 219-0929

7191 Cypress Lake Drive STE 3 #1159, Fort Myers, FL 33907, United States

www.volunteerbadge.com

This document describes controls in effect as of July 2026 and is updated as the platform evolves. It is provided for evaluation purposes and does not constitute legal advice or a contractual guarantee. FCRA guidance herein is educational; organizations should consult their own counsel on compliance obligations.