SECURE FUNDER™

Certification Requirements — What to Expect

Purpose

To confirm that systems housing merchant data have safeguards in place to limit or mitigate unauthorized external sharing.

Application & Timeline

Organizations are listed in the directory immediately upon applying to signal intent.

> **Requirements do not need to be met at the time of application.**

Verification must be completed within 90 days of application. Extensions available under special circumstances.

Certification Guarantee

Certification is not guaranteed. Participants that do not satisfy all requirements will be removed from the directory. Those that pass are added to the verified directory.

How It Works

Verification is completed through the online self-guided portal. For each requirement, you will answer a series of questions and upload specific evidence (screenshots and screen recordings) demonstrating your controls are active and working. All submissions go through a final review before certification is granted.

> **Example pathways are provided to help clarify each requirement. Equivalent controls are accepted, provided they meet the intent of the requirement.**

Payment

The annual membership fee must be remitted before a final review can be conducted.

Final Review

Once verification is complete, Secure Funder™ will conduct a final review. Please allow 1–5 business days for this process. A Results Summary Report will be provided upon completion indicating the status of each requirement and whether additional information is needed or certification is granted.

The review includes an assessment of all portal submissions as well as an independent background check, which may include an Experian business credit report and a review of publicly available information

for any history of documented crimes related to fraud or financial crime.

Implementation Help

If you do not currently meet all requirements and need help, schedule a call with our team for assistance.

Evidence Format

For most requirements, you will be asked to provide two types of evidence:

- **Screenshot** — a static image of the setting or configuration in your admin panel
- **Screen recording** — a short video demonstrating the control working in practice

Verification Requirements

The following sections outline each area of verification. For each requirement, we have listed the specific evidence that will be requested in the portal.

1. Personnel Controls

Organizational policies to limit risk at the human layer.

Background Checks

Documentation confirming background checks are conducted for personnel with access to sensitive data.

If Yes — Evidence Required:

- Blank copy of your background check authorization form
- Screenshot from your provider showing active account or recent checks (redact PII)

Password Policy

A documented password policy or enforcement settings. At minimum, passwords should meet a required length and complexity standard.

If Yes — Evidence Required:

- Copy of password policy or screenshot of admin panel showing enforcement settings (e.g., minimum length, complexity requirements)

Workstation & Screen Security

Screen Lock

A policy or technical setting requiring workstations to lock when unattended.

If Yes — Evidence Required:

- Screenshot of auto-lock timeout setting enabled in device management or admin panel

Camera & Personal Device Exposure (RECOMMENDED, NOT REQUIRED)

Organizations are encouraged to maintain policies or practices that reduce the risk of sensitive merchant information being photographed, recorded, or transmitted from visible screens or workstations. Examples include restricting camera use around unlocked screens, using privacy screens, and training staff not to capture or transmit merchant information through personal devices.

Off-Boarding Process

A process for immediately revoking system access when employees leave or change roles.

If Yes — Evidence Required:

- Offboarding checklist or policy

Remote Access

If personnel access company systems (email, CRM, etc.) outside of the office, controls should be in place to secure that access. You will select from the following (all that apply):

Remote Access Controls (select all that apply):

- **MFA-protected system access**
  → Covered by Email Security and CRM sections — no additional upload needed.
- **Built-in endpoint management (Google Workspace or Microsoft 365)**
  → Screenshot of endpoint management settings in your admin center.
- **Standalone MDM solution (e.g., Miradore, Prey, Island, Intune, Jamf)**
  → Screenshot of MDM dashboard showing enrolled devices.
- **VPN or IP-based access restrictions**
  → Screenshot of VPN or IP restriction configuration.

2. Email Security

If staff have access to emails containing merchant documents, safeguards must be in place to reduce opportunities of misuse.

Multi-Factor Authentication

MFA must be enabled on email accounts used to receive or handle merchant submissions.

If Yes — Evidence Required:

- Screenshot of MFA setting enabled in your email admin panel
- Screen recording of a login showing MFA prompt triggering and being completed

Email Inbox Access

If merchant documents (bank statements, applications, etc.) ever arrive in or get routed to an email inbox — whether sent directly by brokers/merchants or forwarded from an online application — safeguards must be in place. At least one is required:

If your organization does not accept email submissions, upload documented ISO guidelines confirming email is not an accepted intake method.

Email Safeguards (select all that apply):

- **Submissions route directly to CRM (automated)**
  → Screen recording showing a live submission — send a test deal via email, show the submission inbox, then show the deal appearing in the CRM with matching timestamps.
- **Implementation of Aquamark email watermarking tool (alternative providers accepted)**
  → Screen recording showing a live submission with attachments being watermarked in real time upon receipt.
- **Restricted forwarding and personal email access**
  → Screen recording demonstrating that deal-processing roles cannot forward emails with attachments to external or personal domains, and cannot log into personal email accounts on work devices.
- **Other**
  → Describe your safeguard and upload evidence demonstrating it in action.

3. CRM / Portal Security

System-level controls to limit access to merchant data and deter unauthorized distribution.

Multi-Factor Authentication

MFA must be enabled on CRM and portal accounts.

If Yes — Evidence Required:

- Screenshot of MFA setting enabled in your CRM admin panel
- Screen recording of a login showing MFA prompt triggering and being completed

Role-Based Access

Personnel should only be able to access accounts and information required for their role. Sensitive fields (e.g., SSN) should be restricted based on business necessity.

If Yes — Evidence Required:

- Screenshot of your CRM's role list showing that separate roles exist
- Screen recording logging in as two different roles showing that sensitive fields like SSN are visible to one and restricted for the other

Document Access Controls

If documents are accessible within your CRM/portal, safeguards must be in place to limit the ability to distribute merchant documents externally. Select all that apply (at least one required):

Document Protection (select all that apply):

- **View-only access (documents cannot be downloaded)**
  → Screenshot of access settings showing download is restricted, plus screen recording logged in as a user demonstrating documents cannot be downloaded.
- **Document watermarking (Aquamark or alternative provider)**
  → Screen recording showing a document being accessed or downloaded with a visible watermark.
- **Other**
  → Describe your safeguard and upload evidence demonstrating it in action.

User Verification

External user access should be limited to business-relevant users such as developers, accountants, and investors. Explanation is required if other brokerages or funders appear as users.

Evidence Required:

- Screenshot of your CRM user list showing email addresses (redact names and PII — we only need to see the email domains)

4. Document Storage

Controls on secondary storage locations outside your main systems.

If documents are stored outside your main CRM or portal (e.g., Google Drive, Dropbox, OneDrive), you will select which safeguards are in place (all that apply, at least one required):

Storage Safeguards (select all that apply):

- **View-only / restricted access**
  → Screenshot of sharing/permission settings, plus screen recording demonstrating that download or sharing is restricted.
- **Document watermarking (Aquamark or alternative provider)**
  → Screen recording showing a document accessed or downloaded from storage with a visible watermark.
- **Other**
  → Describe your safeguard and upload evidence demonstrating it in action.

5. Outsourcing

Safeguards for third-party and BPO access to merchant documents.

If BPO teams (onshore or offshore) have access to merchant data, you will select which safeguards are in place (all that apply, at least one required):

BPO Safeguards (select all that apply):

- **View-only access (BPO personnel cannot download files)**

  → Screenshot of permission settings for BPO roles, plus screen recording logged in as a BPO user demonstrating download is restricted.

- **Document watermarking before BPO access (Aquamark or alternative provider)**

  → Screen recording showing a BPO user accessing a document with a visible watermark.