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.

Enrollment & Timeline

Organizations are listed in the directory immediately upon enrollment. Requirements do not need to be met at the time of enrollment. Verification must be completed within **90 days** of enrollment. Extensions available under special circumstances.

Certification Guarantee

Certification is not guaranteed. Participants must meet all program requirements.

How It Works

Verification can be completed via live screen share or through the online self-guided portal. All submissions go through a final review before certification is granted.

Payment

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

Final Review

Upon completion of verification, Secure Funder™ will conduct a final review to confirm that the business is actively registered and in good standing with the Secretary of State, and that there are no past or pending lawsuits involving data misuse.

Verification Requirements

The following sections describe each area of verification. For each requirement, we've listed common approaches used to meet the standard. You only need to demonstrate **at least one** safeguard.

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.

Password Policy

A documented password policy or enforcement settings.

Workstation & Screen Security

A policy requiring screen lock and restricting personal cell phone use where customer data is visible.

Off-Boarding Process

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

Remote Device Management

If employees access merchant data or systems remotely, the organization should have the ability to manage those devices (e.g., Intune, Jamf, Kandji).

2. Email Security

Safeguards to deter unauthorized sharing of email submissions containing sensitive documents.

Multi-Factor Authentication

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

Email Submission Handling

If submissions are accepted via email, safeguards must be in place to deter unauthorized sharing. The goal is to ensure staff cannot freely download unprotected attachments from the submissions inbox and forward them to external parties.

At least one of the following (or an equivalent control) must be in place:

- Submissions are routed directly to your CRM without human intervention
- Inbound attachments are watermarked to deter misuse before human handling (any watermarking provider may be used)
- Download controls or DLP policies limit the ability to transfer submission files externally

If your organization does not accept email submissions, provide documented guidelines or system settings confirming email is not an accepted intake method.

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.

Role-Based Access

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

Document Access Controls

If documents are accessible within your CRM and/or portal, safeguards must be in place to deter unauthorized distribution.

At least one of the following (or an equivalent control) must be in place:

- Files are view-only and cannot be downloaded
- Documents are watermarked to deter misuse before entering the system or at time of download (any watermarking provider may be used)
- Download controls or DLP policies limit the ability to transfer files externally

User Verification

CRM users must be from your organization. No external entities — such as brokerages, software platforms, or other lending companies — should have access.

If related entities have access, the business rationale will be reviewed to determine whether it meets the intent of the requirement.

4. Document Storage

Secondary Storage

If documents are stored outside your main systems (e.g. Google Drive, Dropbox), access controls or sharing restrictions should be in place to limit the risk of unauthorized distribution.

5. Outsourcing

Third-Party Access

If BPO teams (on or off-shore) have access to merchant documents, safeguards must be in place to deter unauthorized distribution.

At least one of the following (or an equivalent control) must be in place:

- BPO personnel have view-only access and cannot download files
- Documents are watermarked to deter misuse before third-party access (any watermarking provider may be used)
- Download controls or DLP policies limit the ability for BPO personnel to transfer files externally