SECURE FUNDER™

Verification Session Guide — What to Expect

Overview

Your verification is a brief, structured walkthrough conducted via live screen share. The session confirms that your existing workflows align with program requirements. This guide covers exactly what we'll review so you can prepare.

Format	Live screen share via Google Meet
Duration	15–30 minutes
Recording	Sessions are never recorded. All information is confidential.

Any member of your organization with appropriate system access may conduct the session. Your representative shares their screen — we do not access your systems directly. Sessions may be paused or rescheduled at any time. The objective is to work with you to achieve certification.

Verification Requirements

The following sections describe each area reviewed during your session.

1. Email Security

Preventing unauthorized access to emails containing sensitive submissions.

Multi-Factor Authentication

MFA must be enabled on email accounts.

> ✔ **How we verify:** While sharing your screen, log out of your email and log back in. We confirm a multi-factor prompt (authenticator app, SMS, push notification, etc.) is triggered before access is granted.

Email Submission Handling

If submissions are accepted via email, your verification follows whichever path matches your workflow:

Option A: Automated Processing

Submissions are routed directly to your CRM without human intervention.

> ✔ **How we verify:** We send a test submission to your intake address in real time and confirm it arrives in your CRM automatically, without manual handling.

Option B: Email Watermarking

Inbound submissions are watermarked before human handling.

> ✔ **How we verify:** We send a test submission with a PDF attachment to your intake address in real time and confirm the attachment is watermarked upon arrival. If you're interested in this route and don't yet have a solution, we can walk you through **Aquamark's email watermarking gateway**.

Option C: Download Controls

If documents can be downloaded without watermarking, the organization must have controls that prevent personnel from transferring submission files to personal email accounts or other unauthorized external destinations.

> ✔ **How we verify:** While sharing your screen, show the controls in place to prevent exfiltration. This may include email forwarding restrictions, blocked access to webmail on workstations, DLP policies, endpoint restrictions, download controls, or other verifiable safeguards.

If your organization does not accept email submissions: We review your documented guidelines or portal/API settings confirming email is not an accepted method.

2. CRM / Portal Security

System-level controls to ensure access is limited to what's needed.

Multi-Factor Authentication

MFA must be enabled on CRM and portal accounts.

> ✔ **How we verify:** While sharing your screen, log out of your CRM and log back in. We confirm a multi-factor prompt is triggered before access is granted.

Role-Based Access

Personnel can only access accounts and information required for their role. Sensitive fields (e.g. SSN) are restricted based on business necessity.

> ✔ **How we verify:** Using admin access, log in as users in various roles while sharing your screen. We confirm that sensitive fields (SSN, DOB, etc.) are hidden or restricted for roles that don't require access.

Document Access Within CRM

If documents are accessible within your CRM, one of the following must apply:

Option A: View-Only

Files can be viewed but not downloaded.

> ✔ **How we verify:** Open a merchant record and attempt to download a document. We confirm the download option is not available or is blocked.

Option B: Watermarked Files

Documents are watermarked before entering the system or at time of download.

> ✔ **How we verify:** Open or download a document from a merchant record. We confirm the file is watermarked with identifying information.

Option C: Download Controls

If documents can be downloaded without watermarking, the organization must have controls that prevent personnel from transferring files to personal email accounts or other unauthorized external destinations.

> ✔ **How we verify:** Same as Email Security Option C — show the controls in place to prevent exfiltration, such as email forwarding restrictions, blocked webmail access, DLP policies, endpoint restrictions, or other verifiable safeguards.

User Verification

CRM users must be from your organization. No external entities should have access.

> ✔ **How we verify:** Pull up your CRM's user list. We review it to confirm no external entities have access — particularly brokerages, software platforms, or other lending companies, including those under common ownership.

If related entities have access, we'll discuss the business rationale to determine whether it meets the intent of the requirement.

3. Document Storage

How documents are managed outside core systems.

> ✔ **How we verify:** If documents are stored in secondary locations (Google Drive, Dropbox, shared folders, etc.), show how access is controlled — who has access, whether sharing is restricted, and whether files are encrypted or protected.

Skipped if all documents live within your CRM.

4. Outsourcing

Applicable if BPO teams (on-shore or off-shore) have access to merchant documents.

Option A: View-Only

> ✔ **How we verify:** Log in as a BPO user or show the BPO role's permissions. We confirm files can be viewed but not downloaded.

Option B: Watermarked Files

> ✔ **How we verify:** We confirm documents are watermarked before third-party access by viewing a file as it appears to BPO personnel.

Option C: Download Controls

> ✔ **How we verify:** We confirm controls are in place to prevent BPO personnel from transferring files to unauthorized destinations — such as email forwarding restrictions, blocked webmail access, DLP policies, or endpoint restrictions.

Skipped if your organization does not outsource any processes involving merchant documents.

5. Personnel Controls

Organizational policies to protect data at the human layer. Share copies or display on screen — redactions are acceptable.

Background Checks

> ✔ **How we verify:** Show documentation confirming background checks are conducted for personnel in roles with access to sensitive data.

Password Policy

> ✔ **How we verify:** Show your documented password policy or pull up enforcement settings in your identity provider (complexity requirements, change schedules).

Screen Security

> ✔ **How we verify:** Confirm your policy requires screen lock when away from workstation and restricts personal cell phone use where customer data is visible. Written policy or device management settings work.

Off-Boarding Process

> ✔ **How we verify:** Show your process for immediately revoking system access when employees leave or change roles. A checklist, HR document, or IT procedure is sufficient.

6. Culture & Leadership

We encourage communicating your certification internally — through onboarding, team meetings, or internal communications. Leadership should signal that protecting sensitive information is an operational priority.

> ✔ **How we verify:** This is conversational. We ask how your organization communicates security expectations to staff and whether leadership is visibly engaged in supporting these standards.

Questions? We’re happy to walk through the process before your session.

Secure Funder™ | info@aquamark.io | (415) 500-1117 | securefunder.org