SECURE BROKER™

Certification Requirements — What to Expect

Purpose

To confirm that brokerages have safeguards in place to protect sensitive merchant information from unauthorized use.

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

Once verification is complete, Secure Broker will conduct a final review. Please allow **1–5 business days** for this process. If all requirements are met, certification will be granted and your Secure Broker digital badge will be issued. If any response requires clarification or adjustment, we will identify the requirement and provide 30 days to address and resubmit.

Implementation Help

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

Verification Requirements

The following sections outline each area of verification. For each requirement, we've listed common approaches organizations may use to meet the standard. Applicants only need to demonstrate **at least one** safeguard per requirement. Alternative methods will also be accepted, provided they meet the intent of the requirement.

1. Funder Vetting

Because brokers share merchant data with third-party funders, vetting those partners is a critical layer of protection.

Funder Evaluation Process

The organization should have a documented process—formal or informal—for evaluating funders before sharing merchant data with them.

Example Pathways

- A review of the funder's online presence, reputation, or industry standing
- Partner interviews or references
- Verification that the funder has a physical address, active business registration, or relevant licensing
- Preference for funders that hold credentials (e.g., Secure Funder™, SOC 2)

2. 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.

Example Pathways

- Upload copy of background authorization form
- Screenshot(s) of background check software, signed in

Password Policy

A documented password policy or enforcement settings.

Example Pathways

- Upload copy of password policy
- Screenshot(s) of restrictions/requirements from an admin panel

Workstation & Screen Security

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

Example Pathways

Screen Lock

- Upload copy of policy
- Screenshot(s) of setting enabled

Cell Phone Policy

- Upload copy of policy

Off-Boarding Process

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

Example Pathways

- Upload copy of checklist or policy

Remote Device Management

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

Example Pathways

- Screenshot(s) of settings
- Video(s) demonstrating restrictions for various users

3. Email Security

Safeguards to protect merchant submissions received via email.

Multi-Factor Authentication

MFA must be enabled.

Example Pathways

- Video(s) of MFA prompt triggering upon login
- Screenshot(s) of setting enabled

Submission Handling

If submissions are accepted by email, safeguards must be in place to limit unnecessary access, downloading, or forwarding, ensuring they are not freely transferable outside the organization.

Example Pathways

- Submissions are automatically routed directly into your CRM
- Implementation of Aquamark's email watermarking tool
- Shared inboxes use individual user access rather than shared passwords
- Download controls, DLP policies, or email security settings limit external transfer of submission files

4. CRM / Portal Security

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

Multi-Factor Authentication

MFA must be enabled.

Example Pathways

- Video(s) of MFA prompt triggering upon login
- Screenshot(s) of setting enabled

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.

Example Pathways

- Screenshot(s) of role settings
- Video(s) logged in as various users/roles showing sensitive data redacted or not visible (e.g. SSN)

Document Access Controls

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

Example Pathways

- Files are view-only and cannot be downloaded
- Implement document watermarking so files are watermarked before entering your system, or at the time of download
- Download controls or DLP policies limit the ability to transfer files externally

5. 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.

Example Pathways

- Screenshot(s) of access settings
- Video(s) demonstrating restrictions for various users

6. 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.

Example Pathways

- BPO personnel have view-only access and cannot download files
- Implementation of document watermarking so files are protected before access
- Download controls or DLP policies limit the ability for BPO personnel to transfer files externally

7. Outbound Security

OPTIONAL, BUT RECOMMENDED

Because brokers send merchant documents to multiple third parties, additional precautions at the point of sharing can help maintain chain of custody and deter misuse downstream.

Example Pathways

- Document watermarking before submission to funders
- Secure file-sharing links with download restrictions, expiration dates, or access logging
- Password-protecting documents