SECURE BROKER™

Certification Requirements — What to Expect

Purpose

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

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, but may reapply once and if eligible.

How It Works

Verification is completed through an online self-guided portal. Answer a series of questions and upload specific evidence (screenshots and screen recordings) demonstrating your controls are active.

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

Secure Broker™ will conduct a final review and provide a report showing the status of each requirement, including whether any additional information is needed. The review includes an assessment of the uploaded evidence, verification that the applicant is an active and registered business, and a review of the Experian business credit report. The Experian business credit review is limited to identifying lawsuits related to the misuse of customer data and is not intended to evaluate ordinary commercial disputes.

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.

Example Pathways:

- 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.

Example Pathways:

- 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.

Example Pathways:

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

Off-Boarding Process

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

Example Pathways:

- 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 — e.g., one or more of the following: MFA, endpoint management, MDM solutions, VPN or IP-based restrictions.

Camera & Personal Device Exposure (RECOMMENDED, NOT REQUIRED)

> Organizations are encouraged to maintain practices that reduce the risk of sensitive merchant information being captured using cell phone cameras near workstations.

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 your email system.

Example Pathways:

- 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 merchants or forwarded from an online application — safeguards must be in place. At least one is required:

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 deal 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.

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 your CRM/portal.

Example Pathways:

- 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.

Example Pathways:

- 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.

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.

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.