

United States Postal Service

§ 501.14

§ 501.13 False representations of Postal Service actions.

Providers, their agents, and employees must not intentionally misrepresent to customers of the Postal Service decisions, actions, or proposed actions of the Postal Service respecting its regulation of Postage Evidencing Systems. The Postal Service reserves the right to suspend and/or revoke the authorization to manufacture or distribute Postage Evidencing Systems throughout the United States or any part thereof pursuant to § 501.6 when it determines that the provider, its agents, or employees failed to comply with this section.

§ 501.14 Postage Evidencing System inventory control processes.

(a) Each authorized provider of Postage Evidencing Systems must permanently hold title to all Postage Evidencing Systems which it manufactures or distributes except those purchased by the Postal Service or distributed outside the United States.

(b) An authorized provider must maintain sufficient facilities for and records of the distribution, control, storage, maintenance, repair, replacement, and destruction or disposal of all Postage Evidencing Systems and their components to enable accurate accounting and location thereof throughout the entire life cycle of each Postage Evidencing System. A complete record shall entail a list by serial number of all Postage Evidencing Systems manufactured or distributed showing all movements of each system from the time that it is produced until it is scrapped, and the reading of the ascending register each time the system is checked into or out of service. These records must be available for inspection by Postal Service officials at any time during business hours.

(c) To ensure adequate control over Postage Evidencing Systems, plans for the following processes must be submitted for prior approval, in writing, to PTM:

(1) Check in to service procedures for all Postage Evidencing Systems—the procedures are to address the process to be used for new Postage Evidencing Systems as well as those previously leased to another customer.

(2) Transportation and storage of meters—procedures that provide reasonable precautions to prevent use by unauthorized individuals. Providers must ship all meters by Postal Service Registered Mail unless given written permission by the Postal Service to use another carrier. The provider must demonstrate that the alternative delivery carrier employs security procedures equivalent to those for Registered Mail.

(3) Postage meter examination/inspection procedures and schedule—The provider is required to perform postage meter examinations or inspections based on an approved schedule. Failure to complete the meter examination or inspections by the due date may result in the Postal Service requiring the provider to disable the meter's resetting capability. If necessary, the Postal Service shall notify the customer that the meter is to be removed from service and the authorization to use a meter revoked, following the procedures for revocation specified by regulation. The Postal Service shall notify the provider to remove the meter from the customer's location.

(4) Check out of service procedures for a non-faulty Postage Evidencing System when the system is to be removed from service for any reason.

(5) Postage meter repair process—any physical or electronic access to the internal components of a postage meter, as well as any access to software or security parameters, must be conducted within an approved facility under the provider's direct control and active supervision. To prevent unauthorized use, the provider or any third party acting on its behalf must keep secure any equipment or other component that can be used to open or access the internal, electronic, or secure components of a meter.

(6) Faulty meter handling procedures, including those that are inoperable, mis-registering, have unreadable registers, inaccurately reflect their current status, show any evidence of possible tampering or abuse, and those for which there is any indication that the meter has some mechanical or electrical malfunction of any critical security component, such as any component the improper operation of which