§ 501.11 Reporting Postage Evidencing System security weaknesses.

(a) For purposes of this section, provider refers to the Postage Evidencing System provider authorized under §501.2 and its foreign affiliates, if any, subsidiaries, assigns, dealers, independent dealers, employees, and parent corporations.

(b) Each authorized provider of a Postage Evidencing System must notify the Postal Service within twenty-four (24) hours, upon discovery of the following:

(1) All findings or results of any testing known to the provider concerning the security or revenue protection features, capabilities, or failings of any Postage Evidencing System sold, leased, or distributed by it that has been approved for sale, lease, or distribution by the Postal Service or any foreign postal administration; or has been submitted for approval by the provider to the Postal Service or other foreign postal administration(s).

(2) All potential security weaknesses or methods of tampering with the Postage Evidencing Systems that the provider distributes of which it knows or should know and the Postage Evidencing System model subject to each such method. Potential security weaknesses include but are not limited to suspected equipment defects, suspected abuse by a customer or provider employee, suspected security breaches of the Computerized Meter Resetting System (CMRS) or databases housing confidential customer data relating to the use of Postage Evidencing Systems, occurrences outside normal performance, or any repeatable deviation from normal Postage Evidencing System performance.

(3) Cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on Web sites. Cyber attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm Web sites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access. Cyber security risk disclosures reported must adequately describe the nature of the material risks and specify how each risk affects the Postage Evidencing System.

(c) Within a time limit corresponding to the potential revenue risk to postal revenue as determined by the Postal Service, the provider must submit a written report to the Postal Service. The report must include the circumstances, proposed investigative procedure, and the anticipated completion date of the investigation. The provider must also provide periodic status reports to the Postal Service during subsequent investigation and, on completion, must submit a summary of the investigative findings.

(d) The provider must establish and adhere to timely and efficient procedures for internal reporting of potential security weaknesses and shall provide a copy of such internal reporting procedures and instructions to the Postal Service for review.

(e) Failure to comply with this section may result in suspension of approval under §501.6 or the imposition of sanctions under §501.12.

§ 501.12 Administrative sanctions.

(a) An authorized Postage Evidencing System provider may be responsible to the Postal Service for revenue losses