

CENTRALIZED RECEIVABLES SERVICE (CRS) TECHNICAL BULLETIN

Number 21-05
April 26, 2021

POD and Security Breaches

Proof of Debt (POD) documents provide the debtor with proof that they owe the debt for which they are being billed. CRS encourages agencies to upload POD during case creation. Providing POD with the demand letter eliminates the need for debtors to request POD separately, prolonging the collection process. Debtors who are provided POD immediately tend to resolve their debt sooner.

The main cause of Security Breach incidents is POD documents being uploaded to the wrong debtor's case; therefore, it is imperative that all agency users closely review documents prior to uploading them and again before finalizing the case. Users must ensure all documents are accurate and belong to the debtor for whom the case is being created.

In the event of a Security Breach, both the Fiscal Service Information System Security Officer (ISSO) and the agency's management will be notified immediately. Once notified, the agency is responsible for:

- 1) reporting the security breach according to the agency's internal security protocols, and
- 2) notifying the affected individual that their Personal Identifiable Information (PII) was compromised.

CRS users should upload POD when creating a case. Users are responsible for ensuring all uploaded documents belong to the correct debtor and are redacted to eliminate exposure of PII. For instructions on how to upload POD when creating cases, and for information on how to delete erroneous documents prior to creating a case, see *Adding Documents During Case Creation* in the CRS User Guide. See *Handling Personal Identifiable Information* in the CRS User Guide for information on identifying and redacting PII.

For additional information regarding PII, POD, and/or security breaches, please contact CRS Agency Relations by calling your Program's IVR Number and selecting Option 5, or by emailing crsagencyrelations@usbank.com.

<end>