Protecting Personally Identifiable Information:
Your Responsibility as a Chapter 7 Trustee

By Doreen Solomon, Assistant Director for Review and Oversight
Executive Office for U.S. Trustees

Personally Identifiable Information

As Chapter 7 trustees, you receive sensitive personal information about the debtors whose cases you administer. The loss or improper dissemination of personal information can have significant consequences. While the *Handbook for Chapter 7 Trustees* sets forth various policies designed to help you protect sensitive information from loss or unauthorized disclosure, ultimately you, as trustee, are responsible for ensuring that this information is protected. Accordingly, we recommend that you actively take steps to protect debtors' personal information from accidental or unauthorized disclosure.

In consultation with the NABT, the Program is formulating additional policies to supplement those that are currently in the *Handbook for Chapter 7 Trustees* on protection of sensitive information. We expect these policies to take effect by the fall of 2009. This article discusses the means by which you can minimize the risk of losing debtors' personally identifiable information (PII) and the steps to take if there is a loss or potential loss of PII. Note that privacy protections vary from state to state and, therefore, you should consult applicable state law to determine if additional actions are necessary.

In May 2007, the Office of Management and Budget (OMB) released a memorandum on agency responsibility to safeguard against, and respond to, the breach of PII. In the memorandum, OMB defines PII as information that can be used to distinguish or trace an individual's identity, such as "name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[1] The OMB definition of PII is adopted for purposes of this article.

The sources of debtor PII, which are typically the debtor's bankruptcy schedules, tax returns and pay advices, may be transmitted to you electronically or in hard copy. You, in turn, may store all or part of the debtor's information electronically or in hard copy.[2] Each of these forms of data storage presents its own risks when it comes to accidental or unauthorized disclosure or loss of PII.

---

[1]To read the full text of the OMB Memorandum, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* go to www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

[2] In January 2006, the U.S. Trustee Program issued guidance to trustees governing the storage, access and disposal of debtor tax returns. A copy of that guidance may be obtained from the U.S. Trustee's office.

Minimizing Risks of Data Loss

An intrusion into your computer system or theft of a laptop presents an obvious opportunity for data loss from your electronically stored records. The *Handbook for Chapter 7 Trustees* discusses some of the measures you should have in place to minimize the risk of data loss, such as keeping computer hardware and software in a secure, limited access area; ensuring that only authorized users have access to the chapter 7 computer programs and data via the terminal, network, or modem; and storing all estate files, including paper and electronic accounting records, in secure facilities that are not accessible to the public.

Working from home, as well as transporting data and documents to and from home or section 341 meetings, also present the opportunity for data loss and unauthorized disclosure. Documents and data files containing debtor PII and/or trustee financial information should be secured or within the trustee's control. If the trustee or an employee works out of a home office, all information containing PII should be stored securely. Unauthorized individuals should not have access to this information at any time.

The value of data security measures can be severely compromised if your employees do not understand their responsibilities as users of the computer system. It is recommended that you implement "rules of behavior," which explain the employee's responsibilities as a user and the penalties for noncompliance. Rules of behavior should include provisions designed to minimize the introduction of viruses, worms and other malware, such as prohibiting employees from downloading software or changing configurations and/or settings of the operating and security systems, and warning employees not to open emails from suspicious sources or visit untrusted Web sites. Further, to minimize the risk of unauthorized intrusions, the rules of behavior may limit employees' use of office computers for personal email and instant messaging.

Additional risks of data breach come from using mobile computing devices and accessing data remotely. The use of wireless networks to access chapter 7 trustee data is prohibited at this time. The Program will be working with the NABT to develop a policy to address remote communications including the safeguarding of data stored on a laptop, flash drive or other computing device. Until this policy is in effect, the Program recommends that data stored on remote computing devices be protected from accidental or unauthorized disclosure if the laptop, flash drive or other computing device is lost or stolen. There are two types of protection to be considered: protection of the device itself and protection of the data stored on the device. To prevent someone who has found or stolen your laptop from accessing data, you should have a Basic Input-Output System (BIOS) password to access the laptop and, where available, the laptop should have a password for the hard drive. In addition, the laptop hard drive should be encrypted so the data is not useable by intruders. Flash drives and other mobile storage units containing trustee data should also be encrypted. If the storage media does not support encryption, the trustee should encrypt the data before storing it.

Reporting Loss of PII

While the opportunity for loss or potential loss of PII will be greatly minimized by following the practices discussed above, in rare cases, loss or potential loss may occur. Program policy will include the following guidelines, which apply when a trustee loses electronic or paper files containing PII:

- Immediately (within 24 hours after discovery, if possible) report the loss or potential loss to the U.S. Trustee or U.S. Trustee's representative.

- The report, which may be by telephone or email, must summarize the known facts relating to the breach and any actions taken in response.

- Depending upon the circumstances, report the loss or potential loss to local law enforcement and to your insurance carrier.

The course of action followed and level of notification to affected individuals will be determined based on the risk the data breach poses to the individuals, in accordance with state privacy laws. For example, if a debtor's Social Security number is compromised, you may be required to take additional follow-up actions such as providing a debtor with free credit reports for a specified period.

Conclusion

As a Chapter 7 trustee, you are well accustomed to maintaining strict internal controls to protect the estate funds you administer. The PII in your possession is entitled to the same level of protection.