Protecting Personally Identifiable Information:
Your Responsibility as a Trustee

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

Personally Identifiable Information

As chapter 13 trustees, you are entrusted with the sensitive personal information of the debtors whose cases you administer, just as you are entrusted with their payments to creditors. The loss or improper dissemination of personal information can have significant consequences. Accordingly, trustees must actively take steps to protect debtors' personal information from accidental or unauthorized disclosure.

In consultation with the NACTT, the Program is finalizing revised policies on remote access, protection of data, employee rules of behavior, and loss of data. We expect these policies to take effect in 2009. In the meantime, this article discusses the means by which trustees can minimize the risk of losing debtors' personally identifiable information (PII), and the steps they should take if there is a loss or potential loss of PII. Note that privacy protections vary from state to state, and therefore trustees 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 May 2007 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] In addition, other information that is not generally considered PII may need to be protected from loss. Such information includes: country, state or city of residence; age (especially if not specific); gender or race; and name of school a person attends or workplace, grades, salary and job position. When multiple pieces of information of this type are brought together, they may uniquely identify a person.

Trustees receive numerous pieces of PII from the debtors whose cases they administer. The sources of debtor PII, which are typically the debtor's bankruptcy schedules, tax returns and pay advices, may be transmitted to the trustee electronically or in hard copy. The trustee in turn may store all or part of the debtor's information electronically or in hard copy.[2] Each of these

---

[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

forms of data storage presents its own risks when it comes to accidental or unauthorized disclosure or loss of PII. This article will focus on the risks associated with the accidental or unauthorized disclosure of information maintained electronically.

Minimizing Risks of Electronic Data Loss

An intrusion into the trustee's computer system presents an obvious opportunity for data loss from the trustee's electronically stored records. The *Handbook for Chapter 13 Standing Trustees* discusses computer security measures the trustee must have in place, such as securing the server in a locked room and limiting access to the trustee's database by outside parties. The U.S. Trustee Program routinely approves expenses associated with firewalls and other security measures to protect trust data from unauthorized access.

The value of data security measures can be severely compromised, however, if the trustee's employees do not understand their responsibilities as users of the trustee's computer system. Trustees should implement "rules of behavior," which explain the employee's responsibilities as a user and the penalties for noncompliance. Trustees who have an information technology specialist on staff, belong to the Standing Trustee Alliance for Computer Security (STACS), or use the services of an outside computer consultant, may have already implemented rules governing employee use of the trustee's computer system. 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.

Trustees who access their data remotely face additional risks of a data breach. In May 2007, the Program issued guidance on the technical requirements for accessing data remotely from the court room or 341 hearing room.[3] Recently, STACS issued guidance addressing the broader remote access environment. Trustees who belong to STACS may review this guidance on the STACS Web site at www.stacs.net.

The Program is developing 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 trustees who store data on remote computing devices take steps to ensure that the stored data is 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

---

the U.S. Trustee's office.

[3] The remote wireless policy and technical requirements can be found on the Program's Web site at www.usdoj.gov/ust/eo/private_trustee/library/chapter13/index.htm.

be considered: protection of the device itself and protection of the data stored on the device. To prevent someone who has found or stolen a trustee's laptop from accessing data, the trustee 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 if a trustee follows the practices discussed above, in rare cases loss or potential loss may occur. Program policy will include the following guidelines, which apply when the trustee loses electronic or paper files containing PII:

- Immediately (within 24 hours after discovery, if possible) the trustee must 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, the trustee may also need to report the loss or potential loss to local law enforcement and to the trustee's insurance carrier.

The course of action that the trustee must follow 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, the trustee may be required to take additional follow-up actions such as providing a debtor with free credit reports for a specified period.

Conclusion

Trustees are well accustomed to maintaining strict internal controls to protect the trust funds they administer. The PII that trustees have in their possession is entitled to the same level of protection. Trustees can ensure that PII is protected by implementing procedures that minimize the risk of unauthorized access to the trustee's data, by providing employees with rules of behavior that govern employee use of trustee computer systems, and by encrypting data that is stored on mobile computing devices.