Office of Chief Counsel
Internal Revenue Service
Memorandum

Number: **201120002**
Release Date: 5/20/2011

CC:PA:07:ALMielke
GL-149712-10

UILC: 6103.01-00

date: February 15, 2011

to: Associate Area Counsel (Indianapolis)
(Small Business/Self-Employed)

from: A. M. Gulas
Senior Counsel, Branch 7
(Procedure & Administration)

---

subject: Tracking the Redisclosure of Personal Information Obtained by the Internal Revenue Service from a State Department of Motor Vehicles

Issues

1. Whether the IRS is subject to the redisclosure provisions within the Driver Privacy Protection Act of 1994 as incorporated into the Indiana Code.

2. Whether paragraph 4 of the standard Government Account Agreement regarding state law notification requirements is necessary in light of the more specific federal authority that governs disclosure and breach notification.

Answers

1. Once an individual's IN BMV record is collected by the IRS for tax administration purposes, it becomes return information under section 6103 subject to very stringent rules protecting the data from unauthorized access or disclosure. Thus, the specific rules regarding access and disclosure set forth within section 6103 preempt the more general rule set forth in the Driver Privacy Protection Act.

2. The IRS follows federal law and OMB guidance concerning disclosure of breach notifications. As a result, paragraph 4 of the standard Government Account Agreement is unnecessary given that the federal authorities governing breach notification supercede the state law breach notification requirements.

Facts

Currently, the IRS is working on a Government Account Agreement (Agreement) with the State of Indiana that will allow IRS personnel computer access to the Bureau of Motor Vehicles (IN BMV) computer database. The state's standard "enhanced" agreement, which allows access to personal information, includes both recordkeeping requirements regarding the redisclosure of such information and consent to an on-site audit of such records.

The IN BMV database contains "Personally Identifiable Information" (PII). The IN BMV is concerned with maintaining the security and privacy of those individuals who have PII in the IN BMV database. The IRS obtains motor vehicle registration and lien information from the IN BMV primarily in the course of performing collection investigations. The information is used to determine whether there is sufficient equity in vehicles to warrant seizure and sale to satisfy outstanding tax liabilities.

The Driver Privacy Protection Act of 1994, 18 U.S.C. § 2721 *et seq*. (DPPA), provides federally imposed restrictions on state motor vehicle bureaus regarding to whom personal information may be disclosed. The DPPA also imposes restrictions on an authorized recipient's redisclosure of personal information.

In reviewing the draft Agreement, you have inquired whether the IRS should have in place safeguards to comply with the redisclosure provision of the DPPA. In addition, you have asked whether paragraph 4 of the Agreement regarding Indiana state law notification requirements is necessary given the more specific federal authority that governs disclosure and breach notification.

Because of the concerns raised by these issues, you have requested that we opine on the matter.

Analysis

Section 6103(a) states that returns and return information are confidential and cannot be disclosed except as authorized by Title 26. "Return information" is defined in section 6103(b)(2) as "a taxpayer's identity,[1] the nature, source or amount of his income…" and includes any "data, received by, recorded by … furnished to, or collected by the Secretary with respect to … the determination of the existence, or possible existence of liability (or the amount thereof) … of any person under this title for any tax…".

[1] Section 6103(b)(6) defines "taxpayer identity" as "the name of a person with respect to whom a return is filed, his mailing address, his taxpayer identification number …, or a combination thereof."

IRS employees may access BMV records for a number of tax administration purposes. For example, they may identify or locate assets to seize to satisfy federal tax liens or identifying assets that would suggest a taxpayer is underreporting the amount of his income. Once the BMV record becomes a part of a tax investigation, *i.e*., is received by the IRS, it is return information subject to very stringent rules protecting the data from unauthorized access or disclosure.

There are exceptions to the general confidentiality rule authorizing the IRS to disclose return information, but Congress included each of these exceptions within the statute after careful consideration as to the need for the disclosure to implement federal programs or further federal interests. For example, section 6103(h)(2) authorizes the IRS to make disclosures to the Department of Justice for use in tax administration investigations such as grand jury investigations into tax fraud or other Title 26 offenses. The legislative history of section 6103 evidences Congressional intent that "the Justice Department is to continue to receive returns and return information with respect to the taxpayer whose civil or criminal tax liability is at issue." GENERAL EXPLANATION OF THE TAX REFORM ACT OF 1976, H.R. 10612, 94th Cong. 2d Sess., 320 (JCT Print 1976). Thus, a BMV record collected by an IRS employee, which now has the characterization of return information, might be disclosed to Justice as part of the tax investigation file and be used as evidence to demonstrate unreported income.

Section 6103's confidentiality requirements are buttressed by criminal and civil sanctions. If an IRS employee knowingly makes an unauthorized access of return information (called a UNAX), that employee can be prosecuted under section 7213A, and, if convicted, face a prison term of up to one year, a fine and loss of employment. An IRS employee who knowingly makes an unauthorized disclosure of return information, if convicted of a violation of section 7213, can face imprisonment of up to 5 years, a fine and loss of employment. In addition, section 7431 creates a cause of action for a taxpayer to sue the United States for damages (including punitive damages) if the taxpayer can prove there was a knowing or negligent unauthorized disclosure of, or access to, his returns or return information.

1. Section 6103 preempts the DPPA to the extent they conflict

The DPPA provides federally imposed restrictions on state motor vehicle bureaus regarding to whom personal information may be disclosed. The DPPA also imposes restrictions on an authorized recipient's redisclosure of personal information.

18 U.S.C. § 2721 (b) provides, in relevant part in regard to the Service's activities, that the state may disclose personal information for the following purposes:

> (1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.

> ….
> (4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

Both of these paragraphs contemplate that a federal agency will need to use the BMV records for its official duties. Regarding redisclosure of personal information, 18 U.S.C. § 2721 (c) provides as follows:

> Any authorized recipient ... that resells or ***rediscloses personal information*** covered by this chapter must keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request. (Emphasis added)

(emphasis added). In turn, Indiana has implemented these federal requirements at IND. CODE § 9-14-3.5-13(d) (1996), which provides that "except for a recipient under section 1O(11) of this chapter, a recipient who resells or re-discloses personal information is required to maintain and make available for inspection to the bureau, upon request, for at least five (5) years, records concerning: (1) each person that receives the information; and (2) the permitted use for which the information was obtained."

The DPPA and IN statute provide restrictions on an authorized recipient's redisclosure of PII. As noted above, section 6103 provides the general rule with respect to confidentiality and disclosure issues related to tax returns and tax return information. Once an IN BMV record is collected by an IRS employee, it has the characterization of return information, subject to very stringent rules protecting the data from unauthorized access or disclosure, including an accounting for certain redisclosures. *See* I.R.C. § 6103(p)(3). Moreover, once the BMV record becomes part of an IRS file, it is subject to the record-keeping procedures for that file. To the extent that the DPPA and IN statute impose conflicting safeguard or record-keeping procedures for the redisclosure of PII (such as access to IRS records by state employees), those provisions are ineffective.

As a general rule, a precisely drawn, detailed statute, will preempt more general remedies. *Jett v. Dallas Indep. School Dist*., 491 U.S. 701, 733-34 (1989)(quoting *Brown v. General Svcs. Admin*., 425 U.S. 820, 834 (1976)). For example, in *Hobbs v. U.S.*, the Fifth Circuit Court of Appeals found that section 6103, which permits disclosure of tax return information in a proceeding pertaining to tax administration, is a more detailed statute and should therefore preempt the conflicting provisions of the Privacy Act, because the Privacy Act provisions are more general. 209 F.3d 401, 412 (5th Cir. 2000). Similarly, in *Simichi v. U.S*., the court noted that if any individual

provision of the Privacy Act conflicts with a corresponding provision in section 6103 than the former must yield. 1998 WL 80188, at *5. *See Lake v. Rubin*, 162 F.3d 113, 115-16 (D.C. Cir. 1998); *Cheek v. I.R.S.*, 703 F.2d 271, 271-72 (7th Cir. 1983).

By analogy, section 6103 contains very strict rules that operate to protect data from unauthorized access or disclosure. In contrast, the DPPA and IN statute, provide more generalized protection procedures with respect to redisclosure of PII. As section 6103 is dedicated entirely to confidentiality and disclosure issues related to tax returns and return information, it will preempt the more general protection provisions offered by the DPPA, and IN statute, at least when, as here, provisions conflict.

If, however, the IN BMV believes that the IRS is misusing IN BMV records, it can report the matter to the Treasury Inspector General for Tax Administration, the office with the authority to perform audits of IRS programs as well as investigate the activities of individual IRS employees. *See generally*, I.R.C. § 7803(d) and Conference Report to Accompany H.R. 2676, IRS RESTRUCTURING AND REFORM ACT OF 1998, 217-225. "Taxpayer returns and return information are available for inspection by the Treasury IG for Tax Administration pursuant to section 6103(h)(1)." *Id*., at 224.

2. Federal notification requirements

Paragraph 4 of the standard Indiana Government Account Agreement provides that "if the Subscriber discloses any personal information, the Customer shall pay the cost(s) of the notice(s) of any and all disclosure(s) of the system security breach(es) in addition to any other claims and expenses for which it is liable under the law." IND CODE § 24-4.9-3-1. The IRS adheres to federal law, including section 6103 and the Privacy Act, as well as OMB guidelines to determine when an individual should be notified that his/her information may have been breached.[2]

As a federal agency, the IRS is not permitted to enter into state Government Account Agreements which include a breach notification provision requiring the agency to absorb the cost of notification for all data breaches of PII. Rather, OMB guidance advises federal agencies to consider the risks of identity theft and other adverse effects and to provide notification when an analysis of the factors indicates that notification is appropriate. Office of Mgmt. & Budget, Exec. Office of the President, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16 (2007). In response, the IRS has implemented notification procedures that follow and meet the requirements of the OMB guidance.

---

[2] Among those responsibilities is that the agency must, *inter alia*, only maintain records that are necessary and relevant to accomplish the agency's purpose; inform the individual of the reason it seeks the information and the agency's uses for such information; publish a notice of the systems of records maintained on individuals; maintain records that are timely, accurate and complete; and, establish appropriate technical and physical safeguards to ensure the security or integrity or confidentiality of such records. *See generally* 5 U.S.C. § 552a(e).

In sum, the IRS has breach notification procedures in place and notifies individuals when there is a risk of identity theft or other adverse effect from data breaches. Moreover, the IRS is required to follow federal authority, such as section 6103 and the Privacy Act, with respect to disclosure and breach notification rather than follow state law procedures.

Please call (202) 622-4570 if you have any further questions.