LJN LAW JOURNAL NEWSLETTERS

Business Crimes Bulletin®

An ALM Publication

Volume 19, Number 10 • June 2012

Update: The IRS Whistleblower Program

Part Two of a Two-Part Article

By Sharon L. McCarthy

Last month, we began a discussion of the Internal Revenue Service's whistleblower program, which Congress enhanced in 2006 with the amendment of Section 7623 of the Internal Revenue Code of 1986 (the Code) and enactment of the Tax Relief and Health Care Act of 2006 (the TRHC Act). Tax Relief and Health Care Act of 2006, Pub. L. No. 109-432, § 406 (2006). The key provisions in Section 7623 changed the steps for submitting a claim, and also altered the award system and other aspects of the program. We continue our look at these changes herein and discuss the program's success to date, as well as proposed improvements to the program.

Awards

Whistleblowers who provide information pursuant to Section 7623(b) are eligible to receive an award of at least 15%, but not more than 30%, of the collected proceeds. I.R.C. § 7623(b)(1). The exact amount of an award is determined by the IRS's Whistleblower Office, and the determination is based on the extent to which the informant "substantially" contributed to the action. *Id.* In very specific circumstances, awards can be less than 15%, and in certain cases entirely disallowed. For example, where the information provided is based on certain public sources, the

continued on page 5

The Fragile Fifth Amendment

Compelling 'Decryption'

By Abraham J. Rein

Equipped with a search warrant or subpoena, and sometimes without either, the government may seize or compel an individual to turn over the contents of a computer or smartphone. But when those contents are encrypted (meaning they cannot be accessed without a password), as most are today, must the owner affirmatively facilitate the government's review by decrypting the data or supplying the password to do so? Few courts have weighed in, but two recent opinions demonstrate the fine factual distinctions that drive the analysis.

Background

Computers and related devices, like smartphones, can store massive amounts of private data. For many people, virtually all of their private information is stored and accessible digitally. Moreover, these devices serve as portals to an even greater accumulation of password-protected information housed in "the cloud." Due to this increased volume of digital storage, as well as reliance on such storage for increasingly sensitive information and increasing sophistication of those determined to get at that information, data privacy has become a paramount concern. The use of passwords (encryption) has correspondingly mushroomed.

When the government seeks to compel a target or criminal defendant to produce or enter a password in order to decrypt a device, the Fifth Amendment is implicated to the extent that: 1) the act is "testimonial"; and 2) the facts about which the act is testimonial might tend to incriminate the witness. An act is testimonial if it requires the witness to reveal the contents of her mind, and in so doing to communicate something — in this case the existence, possession, and authenticity of the data behind the encryption curtain. *See United States v. Hubbell*, 530 U.S. 27, 36 (2000) (testimonial nature of "act of production" in a non-digital context).

Two federal courts recently addressed the Fifth Amendment implications of compelled decryption of digital media, coming to different conclusions. In arriving at those outcomes, the opinions illustrate the delicate analytical line that can stand

continued on page 2

In This Issue

Whistleblowers

continued from page 1

Whistleblower Office may (but is not required to) issue an award that does not exceed 10% of the collected proceeds. I.R.C. § 7623(b)(2). Additionally, the Whistleblower Office may reduce the award if the whistleblower is someone who "planned and initiated the planning that led to the underpayment of tax"; and an award is prohibited if the whistleblower is convicted of a crime arising out of such conduct. I.R.C. § 7623(b)(3). (In his Sept. 13, 2011, letter to the IRS Commissioner, Sen. Charles Grassley (R-IA), a drafter of the new law, noted that "limitations for planners and initiators was intended to apply to the *chief architect* or the *chief wrongdoer*," and criticized the IRS's attempts, in IRM 25.2.2.9.2.13.C, to categorize a whistleblower's role as a "planner and initiator as significant, moderate, or minimal." (emphasis in original; Letter available at www.grassley.senate.gov/about/upload/Shulman-re-IRS-9-13-11.pdf).

On Feb. 21, 2012, the Treasury Department issued regulations relating to the definition of "collected proceeds" for purposes of § 7623(b) whistleblower awards. CFR § 301.7623-1 "Rewards and awards for information relating to violations of internal revenue laws." The regulations define "proceeds of amounts collected and collected proceeds" to include the following:

- Tax, penalties, interest, additions to tax, and additional amounts collected by reason of the information provided;
- Amounts collected prior to the receipt of the information if the information provided results in the denial of a claim for refund that otherwise would have been paid; and
- A reduction of an overpayment credit balance used to satisfy a tax liability incurred because of the information provided.

By its omission, the regulation clarifies that fines are not reward-eligible.

The IRS, in recognition of the sensitivity of taxpayer information, has designed an award-determination administrative proceeding to protect taxpayer privacy while giving the whistleblower an opportunity to participate in the process. The IRS will identify the proceeds collected based on the whistleblower's information, the recommended award percentage, the recommended award amount, and the factors on which that award is based. The whistleblower then will have the option of accepting the recommendation, providing comments based on the summary, or reviewing the detailed recommendation and award recommendation file before submitting comments.

IRM 25.2.2.8 (revised June 16, 2010).

IRS Decision-Making Processes

A detailed discussion of the Whistleblower Office's and the IRS's internal procedures regarding whistleblower claims is set forth in the Internal Revenue Manual (IRM). *See* IRM Chapter 25.2.2 *et seq*. (06-18-2010). Some of the procedures written into the IRM in June 2010 appear to be designed to make it more difficult for a whistleblower to recover an award, and undoubtedly will be subject to challenge in court. For example, the IRS has taken the position that "[c]laims may not be paid under [Section] 7623 (a) or (b)[,] which are based on information which leads to the denial of a claim for refund which otherwise would have been paid." *See* IRM 25.2.2.12 (06-18-2010). In other words, even if a whistleblower provides information that allows the IRS to determine an underpayment of tax, no award will be paid if the taxpayer happens to have a net operating loss or credit that offsets the resulting underpayment. (After this provision was added to the IRM, Sen. Grassley sent a letter to the Whistleblower Office strongly criticizing this position of the IRS. *See* Chuck Grassley, 2010 TNT 128-70 Grassley Calls for Delay in Changes to IRS Whistleblower Program, *Tax Notes Today* July 6, 2010.)

Proposed Changes to the Whistleblower Program

In September 2011, the Government Accountability Office (GAO) issued an audit report concerning the new Whistleblower Program, finding a number of problems with the program since it began on Dec. 20, 2006. GAO-11-683, Tax Whistleblowers: Incomplete Data Hinders IRS's Ability to Manage Claim Processing Time and Enhance External Communication. One of the primary problems is the length of time the IRS takes to resolve a whistleblower claim. The GAO found that, since 2007, the Whistleblower Office had received over 1,300 submissions. As of April 2011, approximately 66% of the claims submitted in 2007 and 2008 were still in process. *Id*. at 8. As of May 12, 2011, the IRS had paid only a small number of awards under the new program. The IRS declined to provide specific information about awards based on disclosure bars pertaining to taxpayer return information. (To date, one cash award under the new rules — in the amount of $4.5 million — has been made public through a whistleblower's attorney. *See* Grassley Says IRS Whistleblower Program Needs More Resources, available at www.iwatchnews.org/2011/09/09/6317/grassley-says-irs-whistleblower-program-needs-more-resources.)

The GAO found that whistleblowers whose claims survive the IRS examination phase — which can take hundreds of days — have to wait several years before the IRS can determine if they are due an award based on the taxpayer's right to challenge an assessment of tax. Further adding to the delay, the IRS does not pay claims until it has collected all proceeds from the taxpayer and the two-year refund period has elapsed. GAO Report at 10.

The GAO made a number of recommendations for improvement, including better tracking of the amount of time it takes to process each whistleblower claim; improved forms for easier collection of information; and better annual reporting to Congress on the process, particularly concerning the length of time claims remain at each step of the review process, the reasons for claim rejection and amounts paid to whistleblowers. *Id*. at 26.

Sen. Grassley commented on the GAO report in a letter to the IRS Commissioner in September 2011. He noted that since the new law has been in effect, the IRS has received

continued on page 6

Sharon L. McCarthy is a partner at Kostelanetz & Fink, LLP in New York.

Whistleblowers

continued from page 5

tips on more than 9,500 taxpayers from 1,400 whistleblowers, while rejecting only 1,300 of those claims. *See* Grassley letter at www.grassley.senate.gov/about/upload/Shulman-re-IRS-9-13-11.pdf, at 1. He urged the IRS to take steps to speed the review process so as to avoid discouraging whistleblowers — who often come forward at great risk to themselves — from filing their claims. To that end, he urged the IRS to improve communication with whistleblowers and their attorneys in order to expedite the processing of claims. *Id*. at 6. He noted that the IRS "previously often had little to no understanding, sympathy or interest in whistleblowers," and stressed the importance of the Whistleblower Office being an independent "advocate for the whistleblower" which should "be raising the alarm if meritorious whistleblower claims are being ignored or overlooked by an IRS office." *Id*. at 3, 4.

Conclusion

If the IRS heeds the recommendations of both the GAO and Sen. Grassley and implements changes to speed the review process, better communicates with whistleblowers and the public generally, and publicizes awards without violating taxpayer secrecy rules, the Whistleblower Program will no doubt gain real traction and prove to be a formidable tool in the IRS's arsenal.

—❖—

Fifth Amendment

continued from page 2

her recorded statements on a prison telephone line, and the fact that the computer was found in her room, outside of its case, and apparently identified on a computer network as "RS.WORKGROUP.Ramona" (Fricosu's first name being Ramona). The Tenth Circuit declined to hear the issue, holding that Fricosu sought an improper interlocutory appeal. 2012 U.S. App. LEXIS 3561 (10th Cir. filed Feb. 21, 2012).

United States v. Doe

Just days after the Tenth Circuit turned away Ramona Fricosu's appeal, the Eleventh Circuit found that the Fifth Amendment barred the government from requiring an individual suspected of sharing explicit materials involving minors to decrypt certain seized hard drives. *United States v. Doe* (*In Re Grand Jury Subpoena Duces Tecum*), 2012 U.S. App. LEXIS 3894 (11th Cir. Feb. 23, 2012). In *Doe*, pursuant to a search warrant, the government seized a number of encrypted hard drives from Doe's hotel room. Unable to crack the encryption, the government served Doe with a grand jury subpoena that required him to decrypt the devices himself. Doe refused to comply and, appearing *pro se*, he — like Fricosu — argued that the subpoena sought to compel a testimonial act that might incriminate him in violation of the Fifth Amendment. The district court held Doe in civil contempt, and ordered him incarcerated.

The Eleventh Circuit reversed. Its decision turned on two holdings. First, the court found that forced decryption of the hard drives would constitute "testimony" for Fifth Amendment purposes, a question that the *Fricosu* court did not reach. Second, the *Doe* court rejected the government's argument that Doe's control of the data on the hard drives was a foregone conclusion and therefore the "testimony" required by the subpoena would add nothing to the government's knowledge. The court reached this crucial conclusion despite the fact that Doe's ownership of the hard drives was not in dispute. "Nothing in the record before us reveals that the Government knew whether any files exist or the location of those files on the hard drives," the court explained. "[W]hat's more, nothing in the record illustrates that the Government knew with reasonable particularity that Doe was even capable of accessing the encrypted portions of the drives."

Practice Pointer: The Crucial Factual Distinction

These cases appear to turn on whether pre-existing, independent evidence mooted the testimonial nature of compelled decryption. Remember that in *Fricosu*, other facts, and the inferences drawn from them, established the defendant's knowledge and control over the encrypted machine and its data; without those facts and inferences the decryption might have been found to be potentially incriminating and therefore protected by the Fifth Amendment. More specifically, the *Fricosu* court found that prison call tapes and the location and network identity of the encrypted machine established that the machine both: 1) contained data about which Fricosu was aware; and 2) was in her control. In *Doe*, by contrast, while it was not disputed that the hard drives at issue actually belonged to the witness-suspect, there was no evidence from which the court could determine that he controlled them or that they in fact contained any data. Thus, for Doe, decryption would be testimonial on these points.

Age-old Fifth Amendment jurisprudence developed in the context of ink-on-paper disputes now must be applied in the digital age. The line between *Fricosu* and *Doe* illustrates the kind of minute factual analysis that likely will drive outcomes. As a corollary, our ability to preserve the privacy of our most personal information becomes less certain than ever.

Epilogue

Two weeks after the district court decision in *Fricosu*, Ms. Fricosu's defense attorney suggested to the press that she may have forgotten her password. Then, just three days after the Tenth Circuit declined to hear her appeal, the entire issue — including whether she remembered the password — was mooted when federal authorities finally succeeded in decrypting the laptop without her help. With that, the possibility of a second circuit court opinion on this crucial issue ended — for now.

—❖—