OCTOBER 2013

Contacts:

Christopher R. Hall
Chair

Nicholas J. Nastasi
Vice Chair

Patrick M. Hromisin
Newsletter Editor

Timothy J. Lyon
Contributor

Matthew J. Smith
Contributor

Meghan Talbot
Contributor

Saul Ewing LLP

White Collar and Government Enforcement Practice

White Collar Watch

The Newsletter of the White Collar and Government Enforcement Practice

Contents

Small businesses beware: IRS deploys "big data" to scrutinize cash transactions

By Timothy J. Lyon

IN BRIEF

- **The IRS has signaled its intent to prosecute more small businesses for relatively low-value tax violations.**
- **In doing so, the IRS has increased its reliance on data-driven analyses of the characteristics of businesses, with a particular emphasis on businesses conducting high volumes of cash transactions.**

Small businesses should take note that Internal Revenue Service ("IRS") examinations and actions are increasing. According to Margaret Leigh Kessler, assistant chief of the Western Criminal Enforcement Section, Tax Division, of the Department of Justice, the IRS has begun prosecuting more tax-related cases in recent years, has increased the number of business tax cases it pursues and has demonstrated a willingness to prosecute matters involving smaller amounts of tax loss. For example, on July 24, 2013, the owner of a home improvement company operating in the Pittsburgh, Pennsylvania area was sentenced to 18 months incarceration and three years supervised release for failing in 2006, 2007 and 2008 to pay over to the IRS taxes withheld from his employees. The amount not remitted equaled roughly $87,500 in total for the three years.

Prosecution of such cases continues a recent IRS trend emphasizing greater scrutiny of small businesses generally, whether they be small corporations, subchapter S corporations or partnerships. While examination of tax returns filed across all business categories increased more than 12 percent in fiscal year 2012 compared to 2011, the greatest areas of increase came in audits of smaller entities, especially flow-through entities. For example, 293 more tax returns belonging to large corporations – i.e., those with assets of $10 million or more – were examined by the IRS. However, the number of tax returns of small corporations that were examined increased roughly five times more than that of large corporations, increasing by 1,467. Subchapter S corporations had an even larger increase in returns examined: 3,139; and the increase in partnerships tax returns examined totaled 2,921.

While the IRS does not reveal exactly how its agents determine which entities to target for examination, the agency runs every tax return through a classified computer program designed to determine the possibilities of collecting more tax revenue through an audit. The program assigns a Discriminant Inventory Function ("DIF") score to every tax return. Returns that receive a higher score are more likely to be audited because, the IRS believes, they are more likely to have misrepresented taxable income.

A recent National Taxpayer Advocate study using confidential IRS data found that DIF scores vary across industries. For instance, construction entities and real estate rental companies have higher scores. So too do small businesses within certain geographic regions, such as Los Angeles and San Francisco, California; Houston, Texas; Atlanta, Georgia; the Maryland suburbs of Washington, D.C.; and the District of Columbia. Higher DIF scores likely result from a variety of causes, such as taking unusually high deductions, claiming inordinately large expenses, and dealing in significant volumes of cash, something common in many small businesses.

The focus on small businesses' handling of cash has also increased, along with prosecutions and examinations. The IRS has instituted a specific new program designed to combat underreporting cash transactions, which it considers to be a failure of many small businesses. In 2008, the IRS obtained broader access to merchants' credit and debit card transaction records, and the IRS has been examining such information alongside that reported on small businesses' tax returns. Where the IRS's data analysis reveals a disproportionately large percentage of receipts originating from credit and debit card transactions, the agency has this year started sending letters to certain small businesses asking that they explain why their cash receipts appear to be so small. Sent to roughly 20,000 businesses thus far, these letters typically begin with the sentence, "Your gross receipts may be underreported[,]" and go on to instruct the businesses to complete a form within 30 days explaining "why the portion of your gross receipts from non-card payments appears unusually low."

With the IRS's increased scrutiny of small businesses, attention to tax compliance is now more important than ever. That is especially true considering: (a) that small businesses with higher DIF scores are less likely than those with lower scores to use a third-party tax preparer, or, if they do, to follow the preparer's advice; (b) the IRS's recent overall conviction rate of roughly 93 percent; and (c) that the average criminal sentence ordered thus far in 2013 amounts to 44 months imprisonment.

Google's scanning of emails may constitute wiretapping: Federal District Court denies Google's motion to dismiss class action lawsuit

By Christopher Hall and Matthew Smith

IN BRIEF

- **In a significant ruling on email privacy, the Northern District of California held that Google's interception and scanning of user emails for the purpose of creating targeted advertisements and user profiles may violate state and federal wiretapping laws.**
- **Employers that monitor employee emails should take note of this decision and its potential implications, but understand that the holding is limited to communications that are "in transit."**

Google, Inc.'s practice of "reading" user emails may constitute wiretapping, according to a federal district judge in California. Last month, Northern District of California District Judge Lucy Koh denied Google's motion to dismiss a class action lawsuit accusing Google of violating state and federal wiretapping laws through its practice of intercepting and scanning user emails in

order to develop targeted advertisements and user profiles. The case is *In Re: Google Inc. Gmail Litigation*, 13-MD-02430-LHK, and the full decision can be found at http://www.privacyandsecuritymatters.com/files/2013/09/Gmail_Litigation_Order.pdf.

The case involves a consolidated multi-district litigation in which plaintiffs are seeking damages on behalf of several classes of Gmail (the email service provided by Google) users and non-Gmail users who sent or received messages from Gmail users. The outcome of the case could have far reaching effects regarding email services and consumer privacy.

In its motion to dismiss, Google argued that scanning the messages did not constitute wiretap violations because the practice falls under an exemption for activities that take place "in the ordinary course of its business." Additionally, Google argued that both Gmail and non-Gmail users either explicitly or impliedly consented to the interception and scanning of the messages through Google's Terms of Service and Privacy Policies. Judge Koh disagreed with both arguments.

With regard to consent, Google argued that by agreeing to its Terms of Service and Privacy Policies, all Gmail users "consented to Google reading their emails." Google further suggested that non-Gmail users impliedly consented to Google's interception when those users sent or received emails from a Gmail user. Google implemented multiple versions of its Terms of Service and Privacy Policies during the period at issue. However, the District Court held that it could not be said that any of the classes consented to such interception and use because the language in each iteration of Google's Terms of Service and Privacy Policies "did not explicitly notify Plaintiffs that Google would intercept users' emails for the purposes of creating user profiles or providing targeted advertising."

Additionally, the District Court ruled that the "ordinary course of business" exemption did not apply because Google's interception of the messages was neither instrumental nor incidental to the operation of its email services. Rather, the District Court found that "Google's interceptions of emails for targeting advertising and creating user profiles occurred independently from the rest of the email-delivery system." This was evident in that the Gmail system allegedly had "separate processes for spam filtering, antivirus protections, spell checking, language detection, and sorting than the devices that perform alleged interceptions that are challenged in this case."

In discussing the narrow application of the "ordinary course of business" exception, Judge Koh observed that "[t]he narrow construction of 'ordinary course of business' is most evident in [wiretap] cases where an employer has listened in on employee's phone calls in the workplace." Judge Koh cited several federal cases supporting the proposition that the "ordinary course of business" is narrowly construed in the employment context to allow employer "eavesdropping" on employee phone calls where the employer provides notice and that "there must be some nexus between the need to engage in the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying service or good."

For employers concerned with a variety of internal employment issues – such as the possibility that employees may be revealing company secrets to competitors – the Court's ruling has limited effect. For instance, neither the federal nor Pennsylvania wiretapping statutes prohibit employers from accessing employee emails stored on the employer's computers and servers. See *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2003). Such actions do not constitute an "interception" under the wiretap laws because the search is not conducted contemporaneously as the communication is in transit.

Nonetheless, Judge Koh's decision provides a roadmap that other courts may choose to follow. The principles she enunciated serve as a framework for determining what email providers may lawfully do to monetize free services and what employers may lawfully do to monitor employee email use.

Federal court confirms broad reading of "willfully" in health care false statements cases: Ignorance of the law is no defense

By Meghan Talbot

IN BRIEF

- **The First Circuit recently confirmed that in prosecutions for false statements in health care matters, a defendant does not have to know that making the statement is illegal to be found to have acted "willfully" under the statute.**
- **This ruling is consistent with other courts' recent broad interpretations of "willfully" under the statute.**

The Court of Appeals for the First Circuit has joined in an emerging trend of federal courts broadly interpreting what constitutes willful conduct in health care matters with its decision in *United States v. Russell*.

In upholding the conviction of a laid-off stockbroker who had failed to report his income from working under the table in an application for government-subsidized health care, the First Circuit made clear that ignorance of the law was no excuse. After submitting renewal forms for three years to continue his coverage, the stockbroker, Rodney Russell, was charged and convicted under 18 U.S.C. 1035, "Making False Statements in Relation to Health Care Matters."

On appeal, Russell relied on the theory that the prosecution did not prove his knowledge of the illegality of his actions (i.e., that lying on the application for health care coverage would run afoul of the law). Russell challenged the trial court's jury instructions, claiming that in order to show that he acted "willfully" under the statue, the prosecution would have to "not only prove that Russell's statements were false and that he knew they were false, but that he also knew that making those false statements was illegal." In making this argument, Russell relied on the Supreme Court's ruling in *Bryan v. United States*, which defined " willful" in a different criminal context as "acting with a bad purpose."

The First Circuit rejected this argument in its August decision, ruling that the same Supreme Court opinion noted that the term "willfully" is "a word with many meanings." As such, the only "willful" act that Russell had to commit for conviction under §1035 was making a false statement while knowing it was false.

In the context of false statements in relation to health care matters, this broad definition of "willful" is consistent with other recent appellate decisions in federal courts. In June, the Ninth Circuit held in *United States v. Ajoku* that the "willfulness" requirement of §1035 simply means "deliberately and with knowledge; proving the defendant knew making the false statement was illegal is not required."

Similarly, in July, the *White Collar Watch* reported on the Seventh Circuit decision in *United States v. Natale*, in which the court upheld another conviction under §1035. The defendant had argued on appeal that the term "willful" should equate to "specific intent" – in other words, that the defendant had the specific intent to deceive a health care benefit program. The Seventh Circuit rejected this argument, noting that it had "refused to find an 'intent to deceive' requirement in 'willfulness' language from other, similarly worded statutes."

Rodney Russell was sentenced to five months in prison and three years of supervised release. Although the *Russell* defendant was a consumer of health care, not a provider, three takeaways are clear from his conviction. First, accurate reporting is crucial when participating in health care benefit programs. Second, providers should pay attention to the continuing trend of federal prosecutions for making false statements in relation to health care matters. Third, Courts of Appeals are narrowing the scope of potential defenses to a charge under §1035. Saul Ewing's White Collar practice will continue to monitor this area closely and will provide updates.

The Saul Ewing White Collar and Government Enforcement Practice

Christopher R. Hall, Chair
215.972.7180
chall@saul.com

Nicholas J. Nastasi, Vice Chair
215.972.8445
nnastasi@saul.com

Jennifer L. Beidel
215.972.7850
jbeidel@saul.com

Andrea P. Brockway
215.972.7114
abrockway@saul.com

Brett S. Covington
202.295.6689
bcovington@saul.com

Jennifer A. DeRose
410.332.8930
jderose@saul.com

Cathleen M. Devlin
215.972.8562
cdevlin@saul.com

Justin B. Ettelson
215.972.7106
jettelson@saul.com

Patrick M. Hromisin
215.972.8396
phromisin@saul.com

Keith R. Lorenze
215.972.1888
klorenze@saul.com

Timothy J. Lyon
412.209.2516
tlyon@saul.com

David R. Moffitt
610.251.5758
dmoffitt@saul.com

Joseph F. O'Dea, Jr.
215.972.7109
jodea@saul.com

Amy L. Piccola
215.972.8405
apiccola@saul.com

Christine M. Pickel
215.972.7785
cpickel@saul.com

Courtney L. Schultz
215.972.7717
cschultz@saul.com

Gregory G. Schwab
215.972.7534
gschwab@saul.com

Nicholas C. Stewart
202.295.6629
nstewart@saul.com

Chad T. Williams
302.421.6899
cwilliams@saul.com