NOVEMBER 2012

**Contacts:**

**Christopher R. Hall**
Chair

**Nicholas J. Nastasi**
Vice Chair

**Courtney L. Schultz**
Newsletter Editor

**Gregory G. Schwab**
Contributor

**Nicholas C. Stewart**
Contributor

**Sarah F. Lacey**
Contributor

Saul Ewing LLP

White Collar and Government Enforcement Practice

# White Collar Watch

The Newsletter of the White Collar and Government Enforcement Practice

Contents



## DOJ and SEC Issue Long-Awaited Guidance on the FCPA

By Christopher R. Hall

On November 14, 2012, the DOJ and SEC issued long-awaited guidance on how they enforce the FCPA. Our clients and readers will find the document, styled *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, extremely useful. In particular, pages 57-65 describe the hallmarks of an effective compliance program. The criteria listed describe the standard to which all companies should aspire. The *Resource Guide* also describes hypothetical transactions, at pages 61-64, and recommends how a company should proceed. In particular, the hypothetical on third-party vetting that begins on page 63 contains facts that arise commonly in the "real world," and provides helpful suggestions for how to proceed. Finally, the *Resource Guide* lists examples of past declinations at pages 77-79 — another good source of guidance for how to proceed when issues arise.

In sum, the DOJ and SEC have done a great service to the industry by their joint publication of the *Resource Guide*. The candor and substance of the guidance document will encourage companies to adopt good compliance practices, and will also serve as a "playbook" for business leaders and their counsel when they discover inadvertent payments prohibited by the FCPA.

## Recent Sentencings of Executives Serve as Reminder of Risks of Responsible Corporate Officer Prosecutions; Risks Grow for Medical Device Companies

By Gregory G. Schwab

The recent sentencings of a number of executives held criminally liable under the "Responsible Corporate Officer" doctrine serve as an important reminder that the government increasingly will hold managers, officers, and in-house counsel at drug and medical device companies to a high standard with respect to over-

seeing the safe manufacture and delivery of drugs and medical devices to consumers.

On October 3, the U.S. District Court for the Northern District of Texas sentenced Gary D. Osborn and his compounding pharmacy company ApothéCure Inc. on two counts each of misbranding, to which both had pleaded guilty. Osborn was sentenced to one year of probation, including 90 days of home detention, and a $100,000 fine. The company was sentenced to five years of probation and a $100,000 fine.

Osborn was charged criminally on the basis of the Responsible Corporate Officer ("RCO") doctrine, which is named after a 1975 U.S. Supreme Court decision that stands for the proposition that a "responsible corporate officer" may be found guilty of a misdemeanor crime under the federal Food, Drug, and Cosmetic Act (FDCA) — e.g., misbranding and adulteration — without any intentional wrongdoing. An executive can be convicted of a crime for conduct in which he was not directly involved and that he did not know was occurring.

Osborn's probation sentence was relatively light, but the underlying facts are noteworthy. One of the drugs ApothéCure compounded is called colchicine, which can be injected intravenously for use in the treatment of back and neck pain related to gout. Compounding typically involves a pharmacist preparing a drug following the instructions of a licensed medical doctor. According to the government, three patients who received colchicine from ApothéCure in 2007 died as a result of a colchicine overdose. An FDA investigation subsequently revealed that other vials from the same lot used for these patients were super-potent (~640 percent of the declared potency on the label). Nonetheless, the defendants did not admit that their product caused the deaths.

Both Osborn and ApothéCure were charged with two counts of misdemeanor misbranding on the theory that the drug label did not include correct dosage information. Osborn admitted that as the owner, registered agent, president, sole director, and pharmacist-in-charge of ApothéCure, he was "the person responsible for the procedures and equipment" and "for ensuring pharmacists and pharmacy technicians were properly trained and supervised in the compounding of drugs." Neither the criminal information nor the agreed-upon facts presented to the court mention that Osborn was aware of any discrepancies with respect to the manufacture of the super-potent drug that allegedly killed the three patients. Nor is there mention that he was aware of specific issues related to inadequate procedures or deficient equipment in the intravenous lab (IV lab) generally. Osborn pleaded guilty to the two counts of misdemeanor misbranding.

We can expect that some type of RCO doctrine prosecution will result from investigations into the compounding pharmacy implicated in the recent national fungal meningitis outbreak.

Recent high-profile RCO prosecutions have involved pharmaceutical executives, and the ApothéCure case shows the risks to compounding pharmacies as well. Next in line for the government's attention is medical device companies.

Late last year, a federal court in Pennsylvania handed down sentences ranging from five to nine months in prison to four former Synthes Inc. officers. All four executives pleaded guilty to one count of the strict liability misdemeanor offense of misbranding and adulteration related to Synthes's off-label promotion of bone cement used in back surgery. The government alleged that from August 2003 through January 2004 Synthes engaged in a rogue clinical trial by training spine surgeons to use the bone cement to treat a type of spine fracture common in the elderly notwithstanding known patient risks and despite the fact that the FDA-approved label warned that the product was not intended for such surgeries. During the illegal "test market," three elderly patients died on the operating table. Last month, the Secretary of Health and Human Services exercised her regulatory authority to exclude the officers from federal health care programs.

The Synthes prosecution may only be the beginning for the RCO-related enforcement actions in the medical device industry. At a recent national conference of the Advanced Medical Technology Association, one of the nation's top health care fraud prosecutors said the government has begun to turn its attention from pharmaceutical companies to the medical device industry. Susan Winkler, former chief of the health care fraud unit in the U.S. Attorney's Office for the District of Massachusetts said, "There's no question there is a new focus" on medical device firms. She noted, "There was some real low-hanging fruit in the pharmaceutical industry." Winkler's office had worked on more than 13 cases in the past 12 years that had resulted in more than $200 million in settlements. Those cases focused primarily on Medicaid rebates, pricing scams, and off- label promotion, and Winkler admitted, "The medical device industry may be a bit harder [to investigate] in its initial phases."

Fraud in medical research is one emerging theme, albeit a new area that the government will need time to learn. Prosecutors will examine whether research is reported fairly and accurately and whether negative results are being suppressed. The government will continue to go after physicians — typically the innovators of medical devices — involved in fraud, according to Winkler. Key considerations in any health care fraud case will remain the risk of patient harm and losses to taxpayers. Giving some guidance to avoid prosecution, Winkler stated that her office had declined prosecutions in cases where companies had made voluntary disclosures, fixed problems they had found, and pledged a "robust and effective corporate compliance program."

# The Future Looks Busy for U.S. Inspectors General

By Nicholas J. Nastasi and Nicholas C. Stewart

With the recent passage of two major pieces of legislation governing health care compliance and Wall Street reform, the Office of the Inspector General is expected to play a larger role in overseeing federal agencies and interacting with private parties to guide behavior. Since the founding of this nation, when General George Washington was informed of the combat readiness of his Continental Army, inspectors general have played an important role in the federal government. The modern inspectors general trace their roots to the late 1970s, a response to the growing size of the administrative state and the Watergate scandal. Their intended purpose was relatively straightforward – root out waste, fraud, and abuse within their assigned agency. Since the 1970s, their duties and numbers have increased with the size and scope of government.

Originally, there were only 12 inspectors general. Today, there are more than 70 such offices, employing more than 11,00 employees (including investigators and auditors). In addition, inspectors general were once relatively focused on the internal workings of their assigned agency. Today, they monitor not only the agency implementing Congress' legislative instructions and programs, but also the participants of these federal programs. As Pamela J. Marple noted in her recent *Bloomberg* column, "IG offices now are increasingly focused outward, beyond the walls of their assigned agencies, and into corporate America." Inspectors general investigate "anyone who has received — or applied for — federal benefit or funds," including companies as well as their investors, trusts, and board members. The result? "[A]n increasing number of private [parties] receive IG subpoenas and are subject to IG audits, investigation, or unfavorable IG reports."

By investigating the private participants of federal programs, inspectors general are supporting and in some cases perhaps duplicating efforts of the agencies themselves. After all, agencies are traditionally understood as the regulators of private parties. However, inspectors general have increasingly interacted closely with the participants of administrative programs – raising questions about compliance, subpoenaing and auditing corporate documents, and negotiating resolutions. While inspectors general do not have the corresponding power, enjoyed by many agencies, to compel testimony or impose civil sanctions, their actions can have a significant impact.

Inspectors general often will refer matters to a federal agency or to the Department of Justice (DOJ). In many instances, an inspector general does not simply refer a matter to the DOJ; rather, as Ms. Marple explains, "the IG office[] become[s] the foundation for investigating a DOJ case." The augmented enforcement role played by inspectors general is underscored by the fact that certain inspectors measure success, at least in part, by the resulting number of civil and criminal actions.

The expanding role of inspectors general is unlikely to be limited in the near future. Recently, the federal government enacted substantial pieces of legislation that will increase its involvement in large sectors of the economy. The Affordable Care Act expanded the rights of inspectors general to access claims and payment databases, as well as to investigate health insurance exchanges. For its part, the Dodd-Frank Wall Street Reform and Consumer Protection Act creates a new inspector general to oversee the Consumer Financial Protection Bureau – itself a creation of Dodd-Frank. As has happened with past expansions in government services, these enactments will make more acute the challenge and necessity of accountability. We should expect the duties and numbers of internal watchdogs to continue to increase as well.

# Split State Supreme Court Decision on Third-Party Access to "Backup" Web-Based Email Highlights Need for Reform of Federal Stored Communications Act

By Sarah F. Lacey

Use of private web-based email hosted by Yahoo!, Google, Microsoft, and similar service providers has grown exponentially over the past decade. It is increasingly common for users of such services to leave their email "in the cloud" on the providers' servers. That is, rather than download email to their personal computers and delete the server copies, as was common through the early 2000s, users now typically leave their email stored on the providers' servers indefinitely and without downloading permanent or archival copies to their personal computers.

Users thus may be surprised to learn that their choice to keep opened emails on providers' servers or to download emails to their own computers can affect the level of protection to which they are entitled under the federal privacy laws. Critically, as illustrated by the South Carolina Supreme Court's recent ruling in *Jennings v. Jennings*, No. 27177, 2012 WL 4808545 (S.C. Oct. 10, 2012), protection under the Stored Communications Act ("SCA") may depend on this non-obvious choice.

## Background

The SCA, also known as Title II of the Electronic Communications Privacy Act ("ECPA"), sets forth the methods by which the government may obtain electronic communications, including email, from providers of electronic communication services ("ECS") and remote computing services ("RCS"). SCA, 28 U.S.C. § 2703. The statute also imposes criminal penalties on one who intentionally and without authorization accesses an ECS and "thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ."

Key to the statutory scheme, "electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an [ECS] for the purposes of backup protection of such communication." ECPA, 28 U.S.C. § 2510(17). Part (A) of this definition is generally understood to refer to copies of emails made by a service provider to facilitate transmission. Part (B), on the other hand, invites interpretive difficulty.

At the threshold, in assessing whether part (B) applies, courts inquire whether the service provider in question offers ECS, RCS, or both types of service. *See* ECPA, 28 U.S.C. § 2510(15) (broadly defining ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications"); SCA, 28 U.S.C. § 2711(2) (defining RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system"). If a provider offers only RCS, part (B) is inapplicable; any emails a user maintains with that provider are not in "electronic storage." Emails stored by an RCS may be obtained without a warrant. *E.g., United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009) (ordering Microsoft to comply with government's subpoena *duces tecum* for emails in defendant's Hotmail account, after ruling that Hotmail is an RCS). *But see Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) (implicitly finding that Hotmail and Gmail provide both ECS and RCS). Assuming a provider offers ECS, courts proceed to determine whether the emails in question are in "storage . . . for purposes of backup protection." With the rapid evolution of technology over the past decade, federal courts have frequently struggled to interpret part (B)'s second requirement. The ECPA fails to define "backup."

The majority of courts considering the issue have determined that emails are protected by the SCA if they remain stored on an ECS provider's servers after delivery to the subscriber. *E.g., Theofel v. Farey-Jones*, 359 F.3d 1066, 1075-77 (9th Cir. 2004) (leading case holding that part (B) "applies to backup storage regardless of whether it is intermediate or post-transmission"); *Strategic Wealth Group v. Canno*, Civ. No. 10-0321, 2011 WL 346592, at *3-4 (E.D. Pa. Feb. 4, 2011) (noting that Theofel represents the majority view); *Pure Power Boot Camp*, 587 F. Supp. 2d at 555 (following *Theofel* where defendant accessed plaintiff's web-based Gmail and Hotmail accounts to review "stored" emails); *cf. Fraser,* 352 F.3d at

114-15 (dicta assuming opened emails retained on providers' servers are retained for backup purposes).

On the other hand, some federal courts have adhered to a narrow technical view of "electronic storage." According to that view, the SCA limits protection to emails stored by the provider prior to delivery to the subscriber and copies of those pre-delivery emails made by the provider for its own backup purposes. *United States v. Weaver*, 636 F. Supp. 2d 769, 770-74 (C.D. Ill. 2009) (opened emails residing on provider's server are not in "temporary, intermediate storage incidental to electronic transmission"); see also *United States v. Warshak*, 631 F.3d 266, 291-92 (6th Cir. 2010) (questioning the *Theofel* court's definition of electronic storage). The *Weaver* court distinguished *Theofel* on the basis of what it perceived to be a critical distinction in email system operation. In dicta, the *Theofel* court had suggested that "An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a 'backup' for the user. On the other hand, users of web-based systems such as Hotmail, the *Weaver* court observed, "default to saving their messages only on the remote system. A Hotmail user can opt to connect an email program, such as Microsoft Outlook, to his or her Hotmail account and through it download messages onto a personal computer, but that is not the default method of using Hotmail." Thus, the *Weaver* court reasoned, "unless a Hotmail user varies from default use, the remote computing service is the only place he or she stores messages." Accordingly, it held that the Hotmail user's opened messages were not stored for backup purposes.

## Web-Based Email Not in "Backup" Storage, According to South Carolina Supreme Court

The *Jennings* case involved a Yahoo! Mail account. After plaintiff Lee Jennings confessed to his wife Gail that he had been corresponding with another woman, Gail confided the news to her daughter-in-law, Holly. Holly hacked into Lee's Yahoo! Mail account by guessing the correct answers to the security questions on his account and changing his password. She then searched his account for the emails Lee described and gave copies of them to Gail for use in divorce proceedings. Lee brought an SCA claim against Holly (and others). The trial court granted summary judgment against Lee on his SCA claim, but the intermediate appellate court reversed, finding that Yahoo! provided ECS and Lee's opened emails were stored "for purposes of backup protection" on Yahoo!'s servers. *Jennings v. Jennings*, 697 S.E.2d 671, 677-79 (S.C. Ct. App. 2010) (following *Theofel*).

One year later, the South Carolina Supreme Court reversed the court of appeals in an unusual 2-2-1 ruling. While the five justices agreed that Lee's opened emails were not in "electronic storage" for purposes of the SCA at the time Holly hacked the Yahoo! account, they could not agree on a rationale. Justice Hearn, joined by Justice Kittredge, held the view that the "plain, everyday meaning" of the term "backup" presupposes the existence of more than one copy of an email. Yet, there was no evidence that Lee downloaded or otherwise copied his emails. Without such evidence of dynamic interaction with Lee's email, Hearn and Kittredge found *Theofel* inapposite and "decline[d] to hold that retaining an opened email constitutes storing it for backup protection." These justices virtually ignored the ECS/RCS inquiry and essentially relied on *Weaver* without discussing the similarities between the Yahoo! and Hotmail email systems.

Chief Justice Toal, joined by Justice Beatty, preferred to abide by the narrow technical reading of "electronic storage" that would exclude from coverage all emails the user has opened. 2012 WL 4808545, at *4, 6 (arguing that § 2510(17) only applies to emails in transmission and copies stored by providers incidental to transmission, thus reading sections (A) and (B) together). These justices argued for rejecting both *Theofel* and *Weaver* because both rules would "lead us down the precarious path" of making "the privacy protections of personal email . . . contingent upon the operation of the email system used." These Justices acknowledged, however, that "[m]uch of the difficulty in applying the SCA to cases such as this arises because of the discrepancy between current technology and the technology available in 1986 when the SCA was first enacted" but felt constrained to "interpret, not legislate" in reaching their decision. Finally, Justice Pleicones wrote separately to emphasize his view that the two types of electronic storage defined in § 2510(17) are distinct types of storage that should be analyzed independently. Justice Pleicones otherwise generally agreed with Justices Toal and Beatty and concurred in the result.

## Potential Impact of *Jennings*

The fractured *Jennings* ruling illustrates the difficulty of applying the ECPA's definition of "electronic storage" when today's

modes of email usage and electronic storage were not contemplated when the statute was drafted. The South Carolina Supreme Court's ruling creates further legal uncertainty for service providers, who already find their disclosure obligations under the SCA differ significantly in different jurisdictions. *Compare, e.g., Pure Power Boot Camp*, 587 F. Supp. 2d at 555-56 *and Jennings*, 697 S.E.2d at 675-77 (treating Hotmail as an ECS) *with Weaver*, 636 F. Supp. 2d at 772 (treating Hotmail as an RCS but not an ECS and ordering disclosure of emails to government without a warrant) *and Theofel*, 359 F.3d at 1070 (acknowledging in dicta that emails stored solely on an RCS are not stored for backup purposes).

As other courts have pointed out, to deny an SCA claim such as Jennings' merely because a user keeps his emails solely on a web-based provider's servers is contrary to the legislative intent to deter hacking and safeguard privacy. *E.g., Cardinal Health 411, Inc. v. Adams*, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008) (finding that "where the facts indisputably present a case of an individual logging onto another's e-mail account without permission and reviewing the material therein, a summary judgment finding of an SCA violation is appropriate").

User frustrations at the uncertainty of the level of privacy protection to which their web-based emails are entitled likely will continue to mount. The sustained growth of cloud computing and development of new electronic communication services guarantee that these issues will arise with increasing frequency unless reforms are undertaken. Notably, the United States Supreme Court declined to take up review of the SCA in *Quon v. Arch Wireless Operating Co.* The badly split *Jennings* opinions may increase the likelihood that the Supreme Court will address these issues in the future.

Without significant legislative action or federal Supreme Court review to keep the ECPA and SCA up to date with current technology, strictly literal readings such as those employed by Justices Hearn and Kittredge and the *Weaver* court likely will continue to erode the protections of the ECPA. Amendments to the ECPA have been proposed in the 112th Congress and are currently before the Senate Committee on the Judiciary. The current proposal would require the government to obtain a warrant to acquire the content of stored electronic communications. It would not, however, address the "backup protection" problem directly, and thus if passed, the amendment may not alleviate the split among the courts.

## 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

**Justin B. Ettelson**
215.972.7106
jettelson@saul.com

**Patrick M. Hromisin**
215.972.8396
phromisin@saul.com

**Sarah F. Lacey**
410.332.8791
slacey@saul.com

**Allison B. Newhart**
215.972.7191
anewhart@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