Medical Device Law: Compliance Issues, Best Practices and Trends

Presented by the
American Bar Association
Health Law Section
ABA Section of Science & Technology Law
and Center for Professional Development
In cooperation with
Association for Advancement of Medical Instrumentation
The Food and Drug Law Institute (FDLI)
Federal Bar Association and
Medical Device Manufacturers Association (MDMA)

American Bar Association
Center for Professional Development
321 North Clark Street, Suite 1900
Chicago, IL 60654-7598
www.abacle.org
800.285.2221

The materials contained herein represent the opinions of the authors and editors and should not be construed to be the action of the American Bar Association Health Law Section, Section of Science & Technology Law or Center for Professional Development unless adopted pursuant to the bylaws of the Association.

Nothing contained in this book is to be considered as the rendering of legal advice for specific cases, and readers are responsible for obtaining such advice from their own legal counsel. This book and any forms and agreements herein are intended for educational and informational purposes only.

Printed in the United States of America.

ISBN-13: 978-1-63425-340-6

UNIFORM CERTIFICATE OF SELF STUDY
ABA SELF-STUDY COURSES

To acquire a Uniform Certificate of Self Study for ABA self-study courses, visit the ABA-CLE Web Site at *www.abacle.org* and click on "MCLE."

CDs, DVDs, ONLINE COURSES, DOWNLOADS, and COURSE MATERIALS
ABA self-study products are offered in a variety of formats. To take advantage of our full range of options, visit the ABA Web Store at **www.shopaba.org**.

Product Code: CE1510MDMCOR

To access the interactive version of these materials, please go to: http://ambar.org/ce1510mdmcor

Medical Device Law: Compliance Issues, Best Practices and Trends

Table of Contents

Evolving Trends and Ethical Issues Involving FCA/*Qui Tam* Enforcement of the Medical Device Industry *(Federal False Claims Act and Qui Tam Litigation)*

Faculty and Author Biographies

Joel M. Androphy is a partner in Berg & Androphy in Houston. He has a nationwide practice defending individuals and corporations in white collar civil and criminal cases, and representing whistleblowers in *qui tam* lawsuits. He is the author of several legal books: *White Collar Crime*, a 4 volume treatise by Thompson/West, and th*e Federal False Claims Act and Qui Tam Litigation* by Law Journal Press.

Yogesh Bahl is a managing director in AlixPartners' Financial Advisory Services practice. He joined the New York office in 2014. He has more than 20 years of experience as an accountant and a financial consultant specializing in forensic reviews, litigation consulting and auditing. Prior to joining AlixPartners, he was a partner with a global professional services firm. Mr. Bahl has conducted global investigations involving financial-reporting errors and fraud, alleged violations of various regulations, misuse of corporate assets and related-party transactions. He holds an M.B.A. in finance and statistics and a B.S. in accounting and international business from New York University's Stern School of Business.

Ali Behbahani, M.D. is a partner on the healthcare team at New Enterprise Associates in Chevy Chase, Maryland. He joined NEA in 2007 and specializes in investments in the biopharmaceutical, medical device, specialty pharmaceutical and healthcare services sectors. Prior to joining NEA, he worked as an intern and later as a consultant in business development at The Medicines Company. He concurrently earned his M.D. from The University of Pennsylvania School of Medicine and his M.B.A. from The University of Pennsylvania Wharton School.

Philip S. Brewster is with Brewster Law Firm LLC in Winnetka, Illinois. His experience includes the representation of healthcare systems, physicians and life science companies. He is professionally active in the Food Drug & Law Institute based in Washington, D.C. and the ABA's Health Law Section. Previously, Mr. Brewster served as corporate counsel to the U.S. subsidiary of Brainlab AG. He is a graduate of Boston College Law School and Syracuse University.

Michael A. Carvin is a partner with Jones Day in Washington, D.C. He focuses on constitutional, appellate, civil rights and civil litigation against the federal government. He was one of the lead lawyers, and argued before the Florida Supreme Court, on behalf of George W. Bush in the 2000 election Florida recount controversy. He received his J.D. in 1982 from The George Washington University and his B.A. from Tulane University in 1978.

Michael E. Clark is special counsel with Duane Morris LLP in Houston. He is assigned to its Trial Practice and Health Care Practice Groups. Mr. Clark is a litigator with experience in administrative, complex civil and white collar defense matters. Before entering private practice, he served as chief of the Criminal Division for the U.S. Attorney's Office in the Southern District of Texas. Mr. Clark is an adjunct professor, currently teaching pharmaceutical fraud and abuse at the College of Pharmacy for the University of Florida.

Lisa W. Clark is a partner at Duane Morris LLP in Philadelphia. Her practice focuses on healthcare law with a specialty in health information technology (HIT) issues and mobile health (mHealth) for hospitals, long-term care providers, physicians and other providers. She established and heads the firm's mHealth Interdisciplinary Group. Ms. Clark graduated from the University of Pennsylvania Law School in 1989, a earned a Master's from Harvard Divinity School and is a graduate of Yale University.

David L. Douglass is a partner with Sheppard Mullin Richter & Hampton LLP in Washington, D.C. He previously served as a Department of Justice trial attorney in the Civil Rights Division, Criminal Section. Prior to that, he served as an assistant U.S. attorney for the District of Massachusetts. Mr. Douglass has taught advanced evidence as an adjunct professor at the George Washington University Law School and trial advocacy at Harvard Law School.

David K. Elder is the vice president of Paraxel in Waltham, Massachusetts.

Stephanie J. Fertig is the research project manager for small business programs in the Office of Translational Research at the National Institute of Neurological Disorders and Stroke in Bethesda, Maryland. She manages

both the Small Business Innovation Research and Small Business Technology Transfer programs. In addition, she also manages the Cooperative Research to Enable and Advance Translational Enterprises program for therapeutic devices and the Brain Research through Advancing Innovative Neurotechnologies Initiative Public-Private Partnership Program. Prior to her current position, she was a member of the Repair and Plasticity cluster in the NINDS Division of Extramural Research. Ms. Fertig has a B.S. degree in chemistry with a major in Physics from the University of Virginia and an M.B.A. from the University of Maryland's Robert H. Smith School of Business.

Matthew R. Fisher is an associate with Mirick O'Connell and co-chair of the firm's Health Law Group in Worcester, Massachusetts. His health law practice includes advising clients with regulatory, fraud, abuse and compliance issues. Mr. Fisher's regulatory advice focuses on complying with requirements of the Stark Law, Anti-Kickback Statute, fraud and abuse regulations, licensing requirements, HIPAA and other regulatory requirements. He earned his J.D. in 2008 from Suffolk University Law School and his B.A. in 2004 from Haverford College.

Andrew Gantt is a partner in the Cooley Business Department and a member of the Life Sciences Practice Group in Washington, D.C. He joined Cooley in 2011 and leads its Health Care and Life Sciences Regulatory Practice. Mr. Gantt's practice focuses on health care and life sciences regulatory counseling, complex transactions and strategic business advice. He is a past chair of the ABA eHealth, Privacy & Security Interest Group, and currently chairs the Web & Technology Committee. Prior to his current position, he was a partner at Latham & Watkins.

Sonali Gunawardhana is of counsel with Wiley Rein LLP in Washington, D.C. She serves as co-chair of the firm's Minority Lawyers Affinity Group. Ms. Gunawardhana has nearly 10 years' experience as an attorney at the U.S. Food and Drug Administration, offering clients detailed and practical guidance on how to avoid and resolve FDA regulatory challenges.

Colleen Heisey is a partner at Jones Day in Washington, D.C. Her practice focuses on food and drug law with an emphasis on product promotion and advertising, compliance counseling, manufacturing practice requirements, product recalls, FDA inspection, competitor issues and enforcement actions. She earned her J.D. in 2002 at The George Washington University, her Master of Public Health in 2006 from The Johns Hopkins University and her B.S. in biology, with dual minors in chemistry and environmental science, in 1999 from Lycoming College.

Sheila Hemeon-Heyer is the founder and president of Heyer Regulatory Solutions LLC in Amherst, Massachusetts. She has 28 years of experience in regulatory affairs. She began her career at the FDA, where she was a scientific reviewer in the CDRH Office of Device Evaluation. She then served as Director of Regulatory Services for Medical Device Consultants, Inc. Ms. Hemeon-Heyer joined Boston Scientific Corporation in 2005 as vice president of Global Regulatory Affairs. She holds a B.S. in biomedical engineering from Boston University, an M.S. in biomechanics from the University of Massachusetts at Amherst and a J.D. from Western New England College School of Law.

Gail Hannah Javitt is of counsel with DLA Piper in Washington, D.C. She provides strategic regulatory advice for leading medical device, pharmaceutical, biological products and dietary supplement companies throughout the product lifecycle. She has published and spoken widely on issues at the intersection of law and science, including FDA regulation of genetic testing, precision medicine and next-generation sequencing. Previously, Ms. Javitt was the Law and Policy Director at the Genetics and Public Policy Center in Washington, D.C., where she was responsible for developing policy options to guide the development and use of reproductive and other genetic technologies.

Joy J. Liu is a partner at Ropes & Gray in Washington, D.C. She advises drug and device companies on a broad range of FDA regulatory matters. Joy has significant experience working on advertising and promotion compliance matters, Hatch-Waxman patent and exclusivity issues, and regulatory risk management. She has also worked on a number of government investigations, helping to defend companies during civil and criminal investigations concerning off-label promotion, recalls, safety reporting and GMPs.

Mary K. Logan is president and CEO of AAMI in Arlington, Virginia. She previously served as chief operating officer and general counsel of the American Dental Association in Chicago. She also serves on the board of directors of the American National Standards Institute and is a member of its executive committee and chair of its Organizational Management Forum. She is a graduate of the University of Wisconsin Law School.

John Manthei is a partner in the Washington, D.C., office of Latham & Watkins and serves as global co-chair of its Healthcare and Life Sciences Practice. His practice focuses on regulatory matters involving the Food and Drug Administration for the medical device, pharmaceutical, biotechnology and dietary supplement industries. Prior to joining Latham, Mr. Manthei served as majority counsel for the U.S. House of Representatives' Committee on Energy and Commerce (1998-2000).

Clinton Royce Mikel is a partner with The Health Law Partners PC in Southfield, Michigan.

Timothy M. Moore is an associate with Shook, Hardy & Bacon L.L.P. in Miami. He conducts internal investigations and counsels companies on the Sunshine Act and compliance matters. He previously served in the legal department of a multinational pharmaceutical company. Mr. Moore also served as a prosecutor in the U.S. Attorney's Office for the Southern District of Florida and the Miami-Dade State Attorney's Office.

Gregory F. Noonan is a partner at Collora LLP in Boston. He represents corporations and individuals in white collar criminal and complex civil matters, including government investigations and securities litigation. Prior to joining the firm, Mr. Noonan served as an assistant U.S. attorney for the U.S. Attorney's Offices in the District of Massachusetts and Southern District of California. In Boston, he was a member of the Criminal Health Care Fraud Unit, where he investigated and prosecuted such matters as Medicare fraud, mail and wire fraud, research fraud, off-label promotion and misbranding. In San Diego, he was a member of the General Crimes Unit, where he handled cases involving border crimes, including drug-trafficking and alien-smuggling.

Maura M. Norden is vice president of medical devices and combination products with Greenleaf Health LLC in Washington, D.C. She has nearly a decade of professional experience providing legal and strategic advice to leading pharmaceutical and medical device companies on a broad range of U.S. Food and Drug Administration regulatory matters. Prior to joining Greenleaf, Ms. Norden served as an associate at Sidley Austin LLP in the Food, Drug and Medical Device Regulatory Practice Group. She received her J.D. from the George Washington University Law School and her B.A. from the University of Virginia.

Justin P. O'Brien is a partner with Collora LLP in Boston. He advises public and private companies, professional service firms, nonprofits, government entities, executives, managers, partners, shareholders and licensed professionals in a variety of industries, including financial services, insurance, software, health care, pharmaceuticals, medical devices, engineering, construction, real estate, telecommunications, government, legal, manufacturing and retail. Before joining Collora in 2005, he served as a law clerk to the Hon. Patti B. Saris on the U.S. District Court and as an attorney at Foley Hoag LLP.

Mauricio F. Paez is a partner at Jones Day in New York. He assists clients in responding to cybersecurity breaches and government cyber investigations, identifying and managing global compliance and liability risks related to privacy and cybersecurity, and developing and implementing information management and governance best practices.

Hemant Pathak is assistant general counsel at Microsoft in Washington, D.C., and has been a member of the company's Law & Corporate Affairs department for 12 years. He currently leads the team providing legal support for Microsoft's U.S. Commercial Enterprise Sales Division. He was previously counsel to Microsoft's Health & Life Sciences and Public Sector Industry Units. Prior to joining Microsoft, he was corporate counsel at Oracle Corporation. Mr. Pathak is a 1991 graduate of Washington and Jefferson College and received his J.D. from the Widener University School of Law in 1994.

Philip Phillips is president of Phillips Consulting Group LLC. He has 34 years' experience in FDA regulation of medical devices, focusing on the development and implementation of regulatory strategies regarding the design, manufacture and marketing of medical devices in the U.S. He previously served as the Office of Device Evaluation's Deputy Director for Science and Regulatory Policy for 12 years. Other prior roles include: Director of Program Operations, Interim Director for the Division of General and Restorative Devices, Deputy

Director for the Division of Ophthalmic Devices, and Chief of the Surgical and Diagnostics Devices Branch in the DOD. Mr. Phillips holds a B.S. in microbiology from the University of Maryland and a M.B.A. from the George Washington University.

Robert "Bob" T. Rhoad is a partner with Crowell & Moring LLP in Washington, D.C. He is a member of the firm's Government Contracts and Health Care Practice Groups and co-chairs the False Claims Act and Health Care Litigation practices. Mr. Rhoad defends companies and corporate executives facing criminal and/or civil government enforcement actions under the federal False Claims Act (including *qui tam* "whistleblower" actions), state false claims laws, and other fraud and abuse provisions. Prior to joining the firm in 2007, Mr. Rhoad spent nine years at a national law firm, where he led its False Claims Act and Health Care Litigation practices. Prior to that, he served nearly six years as a government attorney with the Navy Judge Advocate General's Corps.

John L. Robertson is a supervisory special agent with the Federal Bureau of Investigation in Washington, D.C. He entered the FBI in 1996 after serving seven years in the U.S. Navy. Mr. Robertson served in Chicago, where he was one of the FBI's first 100 cybercrime investigators. He conducted investigations involving hackers, child predators, intellectual property crime and counterintelligence threats. He has also worked in Washington, D.C., targeting terrorists, organized crime groups, foreign intelligence officers and led a specialized surveillance team. Mr. Robertson also spent a year at the FBI Academy developing the agency's Investigative Technology Training Program. Today, he is the primary program manager for domestic and international criminal intellectual property rights matters.

Randy V. Sabett is vice chair of the Privacy & Data Protection Practice Group at Cooley LLP. A former crypto engineer with the NSA, his practice focuses on cybersecurity, privacy, licensing and IP. He has dealt with such issues as risk assessment, corporate liability for privacy and data security, identity management, EU data privacy issues, active defense, medical device security, electronic signatures, state and federal information security laws, automotive cybersecurity and security breaches. He is also an adjunct professor at George Washington University.

Jennifer A. Short is an assistant U.S. attorney for the District of Columbia. Her case load consists of affirmative civil enforcement matters, the majority of which are False Claims Act actions. Before taking on her current role in 2010, Ms. Short practiced in the private sector for 15 years, representing clients in False Claims Act cases, government investigations and commercial disputes.

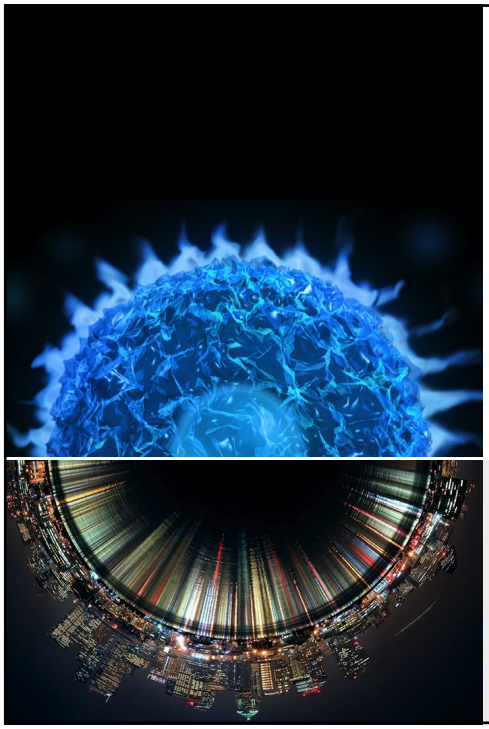
Nancy Singer founded Compliance-Alliance LLC in 2004 to specialize in the professional development for government, association and business professionals. She is on the faculty of George Washington University Medical School and Health Science Program. She has taught classes at Johns Hopkins University, University of Southern California and Harvard Symposia. She presently teaches classes for FDA Staff Colleges and District Offices. Previously, she served as special counsel for the Advanced Medical Technology Association. She began her career as an attorney with the U.S. Department of Justice handling litigation for FDA enforcement cases. She was also a partner at Kleinfeld Kaplan and Becker.

Julie Taitsman is the chief medical officer for the Office of Inspector General for the U.S. Department of Health and Human Services. She is the OIG's primary resource on clinical and scientific issues and lends medical expertise to audits, evaluations, inspections and enforcement actions. She founded and co-chairs OIG's Quality of Care Workgroup. She previously served as senior counsel in the Industry Guidance Branch of the Office of Counsel to the Inspector General. Dr. Taitsman earned a B.A. from Brown University in 1992, an M.D. from Brown University School of Medicine in 1996 and a J.D. from Harvard Law School in 1998.

John Reed Thomas, Jr. is an associate at Gentry Locke in Roanoke, Virginia, and specializes in False Claims Act litigation. Prior to joining the firm, he served as a judge advocate in the U.S. Marine Corps. He is chair of the Federal Bar Association *Qui Tam* Section and writes and lectures on topics related to the False Claims Act.

SECTION A

HOT TOPICS IN MEDICAL DEVICE LAW



OVERVIEW OF CURRENT FDA REGULATORY COMPLIANCE ISSUES AFFECTING MEDICAL DEVICE COMPANIES

2ND ANNUAL
ABA-FDLI-MDMA
MEDICAL DEVICE CONFERENCE

DAVID K. ELDER

PAREXEL CONSULTING

STRATEGIC COMPLIANCE SERVICES

OCTOBER 2015

PAREXEL®
YOUR JOURNEY. OUR MISSION.™

TOP FDA INSPECTION OBSERVATIONS - FY2014

Reference	Short Description	Long Description
21 CFR 820.100(a)	**CAPA**: Lack of, or inadequate, procedures	Procedures for corrective and preventive action have not been [adequately] established. **Specifically,** ***
21 CFR 820.198(a)	**COMPLAINTS**: Lack of, or inadequate ,complaint procedures	Procedures for receiving, reviewing, and evaluating complaints by a formally designated unit have not been [adequately] established. **Specifically,***
21 CFR 820.50	**PURCHASING**: Lack of, or inadequate, procedures	Procedures to ensure that all purchased or otherwise received product and services conform to specified requirements have not been [adequately] established. **Specifically,** ***
21 CFR 820.75(a)	**VALIDATION**: Lack of, or inadequate, process validation	A process whose results cannot be fully verified by subsequent inspection and test has not been [adequately] validated according to established procedures. **Specifically,** ***
21 CFR 803.17	**MDR**: Lack of Written MDR Procedures	Written MDR procedures have not been [developed] [maintained] [implemented]. **Specifically,** ***
21 CFR 820.100(b)	**CAPA**: Documentation	Corrective and preventive action activities and/or results have not been [adequately] documented. **Specifically,** ***
21 CFR 820.90(a)	**NC**: Lack of, or inadequate, procedures	Procedures have not been [adequately] established to control product that does not conform to specified requirements. **Specifically,** ***
21 CFR 820.30(i)	**DESIGN CONTROLS**: Design Changes - Lack of, or inadequate procedures	Procedures for design change have not been [adequately] established. **Specifically,***

ASSESSMENT/DISCUSSION

- **What are the real issues beyond these observations?**
- **Why do the same observations keep showing up year after year?**
- **How should clients be advised to prevent such issues?**
- **What is the appropriate response/reaction if such issues are identified during an inspection?**

WHAT ARE THE REAL ISSUES BEYOND THESE OBSERVATIONS?

- **CAPA (820.100), Complaints (820.198), Nonconforming (820.90), MDR (803)**
  - Detection
  - Investigation/Scope
  - Reaction
- **Purchasing (820.50)**
  - Initial qualification
  - Dealing with issues
- **Validation (820.75)**
  - Missing
  - Failed acceptance criteria
- **Design Changes (820.30(i))**
  - Design Verification and/or Design Validation

WHY DO THE SAME OBSERVATIONS KEEP SHOWING UP YEAR AFTER YEAR?

- **Quality System Inspection Technique (QSIT)**
  - Abbreviated: CAPA + P&PC or Design Controls
  - Comprehensive: CAPA, P&PC, Design Controls, + Management Controls
- **Agency had indicated top reasons for recalls involve issues with Design or Purchased Components.**
- **Investigator tendencies**

HOW SHOULD CLIENTS BE ADVISED TO PREVENT SUCH ISSUES?

- **CAPA**
  - The bellwether system – invest, execute, manage
- **Learn and Evolve**
  - Understand issues/trends in the industry
    - » Subscribe to 483 service
    - » Monitor WLs
    - » Identify industry newsletters of most relevance
  - Understand own operations
    - » Maximize the usefulness of the internal audit and management review
    - » Identify metrics of greatest utility
- **Train/Practice**
  - Peer Review of records, reports, data trending
  - Mock Inspections/SME Preparation/Storyboards

WHAT IS THE APPROPRIATE RESPONSE/REACTION IF SUCH ISSUES ARE IDENTIFIED DURING AN INSPECTION?

- **The reaction to any such issue is generally the same and actually aligns with the CAPA requirements**
  - This is how we will fix the issue (corrective action).
  - This is why the approach taken is the right one (investigation and root cause analysis).
  - This is how long it will take to complete.
  - This is how we will ensure it is effective.
- **Typical difficulties:**
  - Tunnel vision
  - Evidence
  - Risk
    - » Interim Controls
    - » Lookback and Product Impact

Building Workplaces Where Documents Reflect Compliance Initiatives

By Nancy Singer, JD, LL.M

Medical device and pharmaceutical companies make thousands of products that save or improve the quality of lives. Although these products can and do help people, they can also be ineffective or potentially harmful. Employees working for these firms have a strong sense of mission. They are genuinely good individuals who want to make a difference, manufacture safe and effective products and follow the law.

The US Food and Drug Administration (FDA) has detailed regulatory requirements for designing, manufacturing and marketing healthcare products. Companies are required to create standard operating procedures (SOPs) explaining how their firms set up systems to comply with requirements, and then document that employees adhered to those procedures. The companies generally assign these tasks to regulatory and quality assurance (QA) professionals who understand the importance of accurate documentation. Part of the regulatory QA professionals jobs is to educate his or her colleagues on the need for company records to be filled out completely, and signed and dated on the day an activity actually occurred.

During an inspection, an FDA investigator will only view documents. The agency's position is that if an action is not documented, it did not happen. If a company's records are not complete, the investigator will cite the company as being deficient in an official inspection report on Form FDA 483. If FDA finds that the company had numerous deficiencies, the agency can send the company a Warning Letter or institute other forms of regulatory action.

Employees working for companies that manufacture and market healthcare products need to understand that their activities are constantly under a microscope. If a patient is injured, or a company manufactures or distributes unsafe or ineffective products, various entities will behave like sharks, ready to attack the company.

For example, the competition wants to steal the company's market share. Federal prosecutors want to see if the company failed to comply with regulatory requirements and, if so, make an example of it. State prosecutors want to ensure that the company followed all local requirements. If it does not, the company can be assessed large fines to make up budget deficits. Also, plaintiffs' attorneys want to obtain large monetary awards for their clients. Finally, the media often look for negative stories to write about the company.

The Problem

The recession, competition from overseas markets and increased regulatory requirements are factors forcing employees to do more work in less time. Employees running late for a meeting, or interrupted by a phone call can accidentally omit important information in a document. Additionally, frustrated by unexpected network breakdowns or power outages, they may write blunt comments on sticky notes, cryptic emails using inflammatory words, or reports that may not contain all the required information. Most of the time, these documents just remain in the file. However, if a patient is injured by one of the company's products, other parties may gain access to the company's records.

Specifically, FDA could increase its oversight by initiating an immediate inspection or request for more documents during the regularly scheduled inspection. The company could be sued in a product liability action, and then the plaintiff's lawyer would gain access to the company's records. The plaintiff's lawyer will examine the documents to see if he or she can find a statement that might be used to infer inappropriate conduct.

In court, documents speak for themselves. Federal prosecutors can introduce company records as evidence to show that a company distributed products that were not manufactured according to FDA's regulatory requirements. This could subject both the company and the employees to civil or criminal penalties. Plaintiffs' lawyers can use the documents to show that the company's action violated the law, and that the company was negligent or even reckless.

Most corporate interpersonal communication is done by email. Many people, thinking email is private, believe they can be more open. They are wrong. Emails can be considered official documents. Inflammatory terms, incomplete material, missing dates or postdated forms can cause serious problems. The following situations would also be cause for concern in the workplace:

- people writing personal unsupported opinions on issues for which they do not have authority or responsibility
- reports containing inappropriate rationales for why an activity complies with a regulatory requirement
- short emails or statements that are imprecise or do not contain all of the facts
- minutes from meetings reflecting who said what
- handwritten notes on documents

How Should the Problem Be Solved?

Top management must accept that this is a problem. The corporate culture needs to change so that every employee knows that he or she is an ambassador of the firm. They should feel confident that all written communication will reflect the practice of making safe and effective products that comply with all applicable government regulations. Below is a six-step program that will accomplish this goal.

Step 1: Include Appropriate Communication as a Core Value

Top management should review the company's core values to ensure that appropriate communication is included as a practice to which all employees should adhere.

This expectation should be posted on the company's internal website or intranet. The corporate handbook should emphasize that all material written on company computers is the property of the company. Regulatory and QA professionals should institute a program to review SOPs to make sure that they reflect employee practices. Finally, all employees need to commit to following them, not just having them in a binder.

Step 2: Define Expectations and Change Job Descriptions

Management should define the company's expectations and tie the new written communications policies to individual performance reviews.

For example, if employees do not have regulatory authority for specific matters, they should not be injecting personal, unsubstantiated opinions into official reports and records. These employees should share their thoughts, insights and creative solutions in meetings rather than sending dogmatic memos on the subject. Meeting minutes should reflect the reasons for outcomes and results rather than who said what.

Step 3: Educate Employees on Professional Communication.

The regulatory and QA professionals should take the lead in organizing a series of training sessions where all where employees in the company can learn how to write facts, discuss issues and describe actions in a clear way so that the individuals' statements will not be misinterpreted.

Having a lawyer with trial experience conduct the training is a useful strategy. This individual will have credibility and will truly understand how vague or cryptic documents can be used to imply inappropriate conduct.

In putting the training sessions together, the Regulatory and QA professionals should recruit the cooperation and assistance of key company department heads. The department heads can require that employees under their supervision attend one of the sessions, and they can help the lawyer present the content. This sends a strong message that management endorses the program.

The training should not have a lecturer stand in the front of the room reading bullet points from PowerPoint slides. Instead, the training should actively involve all participants in the discussion. The speaker needs to be dynamic and capable of holding an audience's attention.

Techniques to keep everyone engaged include analyzing company documents from the perspective of an FDA investigator or a plaintiff's lawyer. Simulating a trial can be effective, during which volunteers are asked to defend company documents. Exercises in rewriting memos, and the discussion afterward, are also effective teaching tools for improving writing skills.

Another effective method would be to ask the participants to pretend to be witnesses and respond to questioning by:

- the zealous criminal prosecutor attempting to convict a firm of wrongdoing
- an indignant plaintiff's lawyer acting on behalf of someone injured by a firm's product
- a suspicious FDA investigator who is looking for discrepancies from the requirements for which he or she can cite a company
- a skeptical FDA reviewer who needs to determine from a company's application if the data are adequate to allow the firm to market its drugs or devices

During roleplaying, participants learn that lawyers on either side often allow only for yes and no answers with little time to explain in detail. The exercise allows participants to see situations in different ways.

Meanings of terms are fodder for discussion. All employees need to understand the differences between fact and opinion and who within their company would be considered an expert and would be qualified to write an expert opinion on a regulatory issue.

Other techniques include conducting group quizzes about who can be held liable under the *Food, Drug, and Cosmetic Act* and having people explain the consequences of what could happen if procedures are not followed.

The instructor should distribute guiding principles for the use of email and creating good

documentation. Some suggested principles might include:

- Documents last forever.
- People will read your documents with their own agendas.
- If you have authority for regulatory issues or corrective actions, you should provide opinions in writing. If you do not have authority, you should provide the facts to the person who is the decision maker.
- Do not include adjectives with factual statements.
- Provide references to support conclusions.
- Be precise when writing reports.
- Proofread written work by reading it aloud.
- Discuss controversial subjects in meetings rather than through emails.
- Use the phone or communicate in person when written records are not needed.
- Do not send emails when feeling angry.
- Do not use sarcasm in emails.
- Limit using the company email system for personal matters.
- Only provide copies of emails to people who need to know about an issue.
- Do not forward long email chains. People do not want to read them, and they may include inappropriate information.

At the end of the training, the instructor should ask attendees to commit to how they will improve their documentation practices because of the class. Department heads should follow up a few months later, noting improvements and areas still needing work.

Many students taking similar training say they learned how to evaluate their own writing for inflammatory words, allowing some time to pass before writing emails and other types of writing. They also learn to consider the nature of their audience when writing documents.

Step 4: Follow Up After the Training.
The company's management can institute a follow-up program where people collect examples of inappropriate emails or other documentation they received. Identifying information on these documents should be concealed or removed to avoid public embarrassment. Twice a year, each department can hold a training refresher luncheon where people discuss how these documents in the wrong hands could be misinterpreted.

Once a quarter, the company can hold mandatory document clean-up days for the entire staff. On this day, people may come to the office in extreme business casual attire to clear out personal and departmental files of clutter and outdated items. When unsure whether or not to retain items, employees should always check with supervisors. Having a shredder or other document disposal method readily available will help the process.

Other ways to reinforce the message are to display posters, create screen savers or distribute mouse pads with phrases such as "Documents are like diamonds. They are precious, and they last forever."

Regulatory and QA professionals should ensure that, during a company's internal audit, documents that could be misinterpreted are noted. They should take corrective action by encouraging the appropriate person to augment the file with explanatory information, so the situation can be put in context to reflect what actually occurred.

Step 5: Create Procedures for Controversial Issues.
Companies should have procedures for dealing with difficult issues so, when the situation occurs, employees will know what to do.

For instance, if employees have concerns about a product or anything else, the procedure would tell the employee to meet with his or her supervisor about taking corrective action. If the supervisor disagrees and the employee is still unconvinced, the employee should suggest to the supervisor that they go together and talk to people with higher authority or with other disciplines (compliance officers or lawyers) to resolve the issue.

The rationale behind this course of action is if a regulatory decision is endorsed by appropriate functions within an organization, this will ensure that the institution stands behind the decision.

Step 6: Evaluate Performance.
Managers need to follow up, praising or citing people in their performance reviews for how they write. Workers and managers should develop training plans together that would best meet individual or group needs, such as seminars or business writing workshops, for employees needing further guidance.

Conclusion

Companies that manufacture medicines and devices produce inherently risky products. They are not immune to product liability lawsuits. If the program for improving written communications is put in place, employees will be more aware of expectations and better equipped to take ownership of what they include in documents. They will be held accountable for their *actual* behavior, not what others think they did through poorly written emails, memos or other imprecise documents.

Author
Nancy Singer is president of Compliance-Alliance, LLC, a firm that provides training on good documentation practices. Singer's career began as an attorney with the United States Department of Justice where, during a three-year period, she successfully prosecuted seven firms for violations of various criminal statutes. Subsequently she was a partner at the law firm of Kleinfeld, Kaplan and Becker. Singer received JD and LL.M degrees from New York University Law School. Singer is a retired Commander in the United States Naval Reserve. Her email address is nancy@compliance-alliance.com.

SECTION B

ADVANCED ISSUES IN MEDICAL DEVICE LAW

PHILLIPS CONSULTING GROUP, LLC

An Ambiguous Regulation EXPOSED 21 CRF 807.81(a)(3)(ii)

Annual ABA-FDLI-MDMA MEDICAL DEVICE CONFERENCE
October 15-16, 2015
Gibson Dunn, 1050 Connecticut Avenue, N.W.
Washington, DC 20036

Scope of the Discussion

- Most class I and II devices and the few remaining class III devices subject to 510(k) review
- Exclusions - class III devices and certain restricted devices*, including devices:
  - restricted within the meaning of Sections 502(q) and (r) of the FDCA
  - restricted by regulation, e.g., latex condoms
  - restricted through Special Controls, e.g., ultraviolet light absorbing contact lenses

*Aspects of this discussion may still apply

Important Context for Discussion

- The September 2008 statement of Dr. Daniel Schultz before the Senate Special Committee on Aging provides valuable insight into FDA's authority over advertising of medical devices*
- Introducing post-market "claims" in promotion and advertising materials is a FDA regulatory compliance issue that can affect virtually any medical device company
- Enforcement actions based on unauthorized "claims" is a growing regulatory trend

*See http://www.fda.gov/NewsEvents/Testimony/ucm096272.htm

The Ambiguity of 21 CFR § 807.81(a)(3)(ii)

(3) The device is one that the person currently has in commercial distribution or is reintroducing into commercial distribution, but that is about to be significantly changed or modified in design, components, method of manufacture, or **intended use**. **The following constitute significant changes or modifications that require a premarket notification:**

(i) A change or modification in the device that could significantly affect the safety or effectiveness of the device, e.g., a significant change or modification in design, material, chemical composition, energy source, or manufacturing process.

(ii) A major change or modification in the intended use of the device.

Step 1 – Understanding "Intended Use"

- Intended use is a regulatory concept that affords FDA considerable discretion in assessing labeling, promotion, advertising, and device design for compliance with FDA's understanding
  - FDA's definition (21 CFR 801.4)
  - Defined as "...the objective intent of the persons legally responsible for the labeling of devices..."
- Encompasses all aspects of how, for what purposes and under what circumstances the device is intended to be used
- Not always apparent or documented

PHILLIPS CONSULTING GROUP, LLC

5

Step 2 – Determining what is "Major"

FDA's Guidance Document - Blue Book Memo K97-1

- Labeling changes that usually require 510(k)s as per K97-1
  - Most changes in Indications for Use
  - Additions or deletions of "true" Contraindications
  - Reuse of devices previously labeled "single use only"
  - Changes from prescription (Rx) to over-the-counter (OTC) distribution (not vice versa)

PHILLIPS CONSULTING GROUP, LLC

6

Blue Book Memo K97-1 (continued)

- Labeling Changes that do not usually require 510(k)s as per K97-1
  - Changes in Indications for Use that ...
    - limits use to within the currently cleared indication
    - Expands use to a patient population with similar demographics, diagnosis, prognosis, comorbidity and potential for complications
  - Changes in warnings or precautions
  - Attempts to clarify use instructions to make the device easier, safer, or more effective to use.

FDA Regulation of Device "Claims"

- FDA has not defined the term "claim" in the context of device regulation
  - Frequently used synonymously with "intended use" and "indications for use"
  - Often cited by FDA as evidence of off-label promotion
  - FDA has issued no relevant guidance on the subject
- Types of claims
  - Off-label, e.g., claiming clinical benefit in a new patient population
  - Within-label, e.g., espousing the benefits of the on-label use.

Off-Label Claims

Some objectionable claims are easy to recognize

- Examples:
  - A powered aspirators indicated for removal of loose bone chips, blood, or tissue from the body during surgery promoted to be suitable for use in suction lipectomy.
  - A "biliary stent" promoted as being easy to insert into the vasculature
  - An *in vitro* diagnostic assay promoted as a means to determine patient response to drug therapy

Some objectionable claims are not easy to recognize

- Example 1:
  - Indications for Use statement

    Device X is indicated for use as a transitory scaffold for soft tissue support and repair to reinforce deficiencies where weakness or voids exist that require the addition of material to obtain the desired surgical outcome. This includes reinforcement of soft tissue in plastic and reconstructive surgery, and general soft tissue reconstruction.
  - Claims cited as major changes in intended use

    Specific procedures which may benefit from the use of Device X for soft tissue support and repair include:

    - Breast revision surgery, mastopexy with or without augmentation, breast reductions, and muscle flap reinforcement

- Example 2
  - Indications for Use statement

    Device Y provides clinicians with objective measurements of hyperactivity, impulsivity and inattention to aid in the clinical assessment of ADHD. Device Y results should be interpreted only by qualified professionals.
  - Claims representing a new intended use
    - "....monitor response to treatment.."
    - "...objectively measures micro-motion and analyzes shifts in attention state."
    - "Follow-up tests help to assess whether the patient is getting the right intervention."
    - "...optimize treatment in weeks instead of months."
    - "....helps to achieve clinical efficacy sooner."

- Example 3
  - Indications for Use statement

    Device Z is indicated for use in soft tissue approximation for procedures such as general and orthopedic surgery.
  - Claims representing a new intended use
    - "... provides a uniquely simple method for treating the compromised soft tissue of the annulus fibrosus."
    - "... provides a simple, convenient method for treating the compromised soft tissue of the annulus fibrosus."
  - Outcome
    - Adulteration and Misbranding
    - Violation of the IDE regulation and related regulations

- Miscellaneous objectionable claims
  - Representing a device determined to be SE to be "breakthrough"
  - In regard to wound care devices
    - "accelerates wound healing"
    - "results in scarless wound healing"
    - "reduces bacterial colonization"
    - "reduces the need for analgesics"
    - "shortens long bleeding times associated with blood thinners"
    - "barrier may help prevent the risk of infection"
    - "barrier may help decrease the risk of hospital acquired infection"
    - "antibacterial properties when applied to a wound"

Guiding Principles

- Understand the law and regulations, and precedent
- Establish claims substantiation and authorization procedures and document all decisions to proceed without 510(k) clearance
  - Never make a claim that is false or misleading, or has not been substantiated
  - Do not substantively change the FDA authorized Indications for Use without authorization
  - File 510(k)s for claims that expand the patient population beyond the scope of the FDA authorized Indications for Use

Guiding Principles (continued)

- Develop criteria to guide decision-making consistent with the "regulatory risk tolerance" of the company
- Types of claims that may not constitute a major change or modification in intended use may include:
  - Performance and mode of action claims related to the authorized Indications for Use;
  - environmental compatibility; and
  - cost effectiveness

Conclusion

It is unreasonable to believe that all claims require 510(k) clearance making in critical for medical device companies to have procedures and criteria for decision-making to mitigate the risks of encountering enforcement actions related to marketing activities.

Contact Information:

PHILLIPS CONSULTING GROUP, LLC
P.O. Box 39
McHenry, Maryland 21541

E-mail: phil.phillips@phillips-consult.com
Phone: (202) 420-9042

FDA Oversight of Direct-to-Consumer Advertising of Medical Devices (Statement of Daniel Schultz, M.D.)
http://www.fda.gov/NewsEvents/Testimony/ucm096272.htm

SECTION C

INDUSTRY PERSPECTIVE ON PAST YEARS' FDA COMPLIANCE GUIDANCE

JONES DAY | One Firm Worldwide℠

Industry Perspectives on Past Years' Guidance

ABA / MDMA / FDLI Medical Device Law 2015 National Institute

Washington, DC
October 15, 2015

1

Panelists:

- Michael A. Carvin, Partner, Jones Day
- Joy J. Liu, Partner, Ropes & Gray LLP
- Timothy M. Moore, Attorney, Shook, Hardy & Bacon LLP

Moderated by:

- Colleen M. Heisey, Partner, Jones Day

JONES DAY

2

Topics

- Product promotion
- Individual accountability
- Laboratory developed tests
- Mobile medical applications
- Recalls vs. enhancements
- Patient preference and product labeling
- Unique device identifiers

Product Promotion – Evolving Law

- First Amendment cases:
  - *IMS v. Sorrell*
  - *U.S. v. Caronia*
  - *Amarin v. FDA*
  - Filed: *Pacira Pharmaceuticals v. FDA*

Product Promotion – New Frontiers

- Traditional vs. contemporary avenues of promotion
- Healthcare professional- vs. consumer- directed advertising
- Social media
  - FDA:
    - Internet/Social Media Platforms: Correcting Independent Third-Party Misinformation
    - Presenting Risk and Benefit Information
  - Other regulatory considerations

JONES DAY

5

(Not) Product Promotion: Scientific Information

- Scientific/Medical Information
  - Distributing Scientific and Medical Publications on Unapproved New Uses—Recommended Practices
  - Distributing Scientific and Medical Publications on Risk Information for Approved Prescription Drugs and Biological Products—Recommended Practices
- Unsolicited Requests
  - Responding to Unsolicited Requests for Off-Label Information About Prescription Drugs and Medical Devices

JONES DAY

6

Individual Accountability

- September 2015 Department of Justice Memo
  - Cooperation credit eligibility: Corporations must provide DOJ all relevant facts about the individuals involved in the misconduct
  - Investigations should focus on individuals from the investigation's inception
  - Criminal and civil attorneys handling corporate investigations should be in routine communication with one another
  - DOJ will not release culpable individuals from liability when resolving matter with corporation
  - DOJ should not resolve corporate cases without a clear plan to resolve related individual cases before the stature of limitations expires; declinations as to individuals in such cases must be memorialized
  - Civil attorneys should consistently focus on individuals and the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay

JONES DAY

7

Laboratory Developed Tests

- 2012 FDA Safety and Innovation Act
- 2014 Activity
  - Draft Framework for Regulatory Oversight of Laboratory Developed Tests
  - Draft FDA Notification and Medical Device Reporting for Laboratory Developed Tests
  - In Vitro Companion Diagnostics

JONES DAY

8

Mobile Medical Applications

- Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff
- Medical devices that are mobile apps, meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device
  - Mobile apps: software programs that run on smartphones and other mobile communication devices

Recalls / Enhancements

- Distinguishing Medical Device Recalls from Product Enhancements and Associated Reporting Requirements
  - Clarify when a change constitutes a medical device recall
  - Distinguish instances from device enhancements that do not meet the definition of a medical device recall
  - Clarify reporting requirements (Part 806, Medical Device: Reports of Corrections and Removals)
  - “Device enhancement” defined

Patient Preference and Product Labeling

- Patient Preference Information – Submission, Review in PMAs, HDE Applications, and *De Novo Requests, and Inclusion in Device Labeling*
  - What manufacturers and other stakeholders should consider when choosing to collect patient preference information

Unique Device Identifiers

- 2013: Final rule requires device labelers to include a UDI on device labels and packages, except where the rule provides for an exception or alternative
  - Each UDI must be provided in a plain-text version and in a form that uses automatic identification and data capture technology
  - Also be required to be directly marked on a device that is intended for more than one use, and intended to be reprocessed before each use
- Global UDI Database (GUDID); UDI System: Small Entity Compliance Guide; UDI System: Frequently Asked Questions, Vol. 1; Unique Device Identification: Direct Marking of Devices

Thank you

Michael A. Carvin
macarvin@jonesday.com
202-879-7643

Joy J. Liu
Joy.Liu@ropesgray.com
202-508-4691

Timothy M. Moore
tmoore@shb.com
305-755-8924

Colleen M. Heisey
cmheisey@jonesday.com
202-879-3449

SECTION D

FINANCING MEDICAL DEVICES THROUGH CONVENTIONAL AND UNCONVENTIONAL MEANS

Medical Law Device Conference

Financing Medical Devices through Conventional and Unconventional Means

Ali Behbahani

October 2015

The Current State of the Device Market

- **The IPO market for medical device companies remains effectively closed**
  - Only a handful of device companies have gone public – mostly companies that are generating $25M+ in revenues
  - No IPO market for pre-revenue companies
  - Not clear when the IPO market will come back
- **M&A exits have remained relatively steady over the past decade**
  - Innovation at big companies has been stagnant
  - M&A is seen as way to help drive growth
  - Acquisitions are too far and too few in between
  - Many M&A deals are earnout based → only 50% of earnouts typically achieved

The Current State of the Device Market

- **Getting medical devices through market approval has become more difficult**
  - The amount of clinical data required for FDA approval has increased
  - Obtaining sufficient clinical data for reimbursement continues to grow
  - Increased requirements to obtain CE Mark
  - Need to conduct compelling randomized trials to drive physician adoption
- **The capital requirements to fund medical device companies has increased as a result**
  - Due to the lack of an IPO market, VC firms are funding companies for longer periods of time
  - Series E, F, G, etc. and recapitalizations are not uncommon

The Reaction from the VC Community

- **Movement to do later stage deals**
  - 510k project with low clinical risk
  - Approved, revenue-generating companies
  - Build to buy deals with strategics
- **Raising money for early stage deals has become difficult**
  - Many VCs that have traditionally done med tech have stopped doing so
  - Few VCs are actually doing early stage device deals
  - Those that are will do 1 maybe 2 such deals
  - Strategic VCs were picking up the slack but that seems to be decreasing
  - Its not uncommon to speak with 200+ investors in hopes of finding one
- **While things will cycle back and improve, financing are hard to come by**
- **Good projects are still getting funded**

Sources of Capital

- **Bootstrapping**
- **Grant funding and SBIR**
- **Angel / high net-worth funding**
- **Family offices**
- **Traditional VCs**
- **Strategic VCs**
- **Build to buy deals**

Who to Approach

- **There are many VCs….approaching everyone is counterproductive and not feasible**
- **Put together a target list of VCs based on the characteristics of your company/deal**
  - Stage – early stage, later stage, growth equity
  - Sector – biopharma, medical device, healthcare services, HCIT
- **Determine which VCs would be most attracted to your company/deal**
  - Have they done deals at similar stages and sectors are yours?
  - Looking at recent deals in a VCs portfolio is the best way to tell
- **Send an introductory email requesting an initial meeting**
  - Warm intros are better than cold intros
  - Short teaser/deck on the company
  - Best to start with a handful, refine your positions based on feedback and expand outreach

The Process

- **Teaser/deck sent to target VCs**
- **Initial meeting**
  - Usually an hour long
- **Due diligence (4-6+ weeks)**
  - Speaking to physicians or expert
  - Looking through preclinical and clinical data
  - Understanding development plans and capital requirements
- **Partnership presentation**
- **Term sheet**
- **Confirmatory due diligence**
  - IP and any remaining due diligence
- **Legal documentation & closing**

The Initial Meeting

- **Plan for an hour long meeting**
  - ~30 minutes presentation (30-35 slides) & ~30 minutes of Q&A interspersed
  - Send presentation deck beforehand to give your audience a chance to review it
- **What to cover?**
  - Current treatment(s) and unmet need
  - Market potential
  - Product
  - Preclinical and clinical data
  - Regulatory and clinical development path
  - Competitive landscape and IP
  - Reimbursement
  - Management team
  - Financing

Due Diligence Process

- **If a VC firm is interested, they will do due diligence**
  - Help understand where the business is today and where it could be
  - Assess the risks
- **Momentum, momentum, momentum….**
  - It is hard to say how long a venture firm's due diligence will take – weeks or months
  - Having a data room or a set of documents that focus on the key diligence areas can be useful in getting the firm going
  - Checking in every so often can keep things moving forward
  - Deals that lose steam likely don't happen
- **The goal is to get the VC firm to a decision as to whether they would like to invest**
  - A partnership presentation is likely the next hurdle before a term sheet

The Term Sheet

- **Valuation**
  - Often the primary focus, but its just one term
  - Focus on % ownership as opposed to a specific pre-money number
  - A valuation that is too high in this round may make it tougher for you to raise the next round of financing
- **Liquidation preference**
- **Option pool size**
- **Board composition**
- **Protective provisions and voting thresholds**
- **Anti-dilution**
- **Conditions to closing**

General Points of Advice

- **Choosing the right group of VCs to target is key to making the process easier**
  - Use your network to get warm intros but don't be afraid to cold call
- **Persistence is key – you will hear a lot of "no's"**
- **Maintaining momentum during the due diligence process is key to getting to a conclusion sooner rather than later**
- **Have a good idea of how much it will take to achieve key value creating milestones**
- **Help facilitate an investor's due diligence process –**
  - Makes things go faster and the onus is on you to help get the VC comfortable
- **When negotiating the term sheet don't lose sight of the bigger picture**
  - Its not about getting the highest pre-money valuation
  - None economic terms can just as important if not more
- **The closing is just the beginning**

Arnall Golden Gregory LLP
Attorneys at Law

Financing Medical Devices through Conventional and Unconventional Means

Michael E. Burke
October 15, 2015

Funding Options

- Conventional and Otherwise:
  - 'Traditional' VC funding.
  - Grant and other Non-Dilutive Funding.
    - Federal and State Options (Third Frontier/Ohio; Ben Franklin Technology Partners/Pennsylvania).
  - Corporate venturing.
    - Seeking capital from established corporations in exchange for a purchase option.
    - Funding from outside the device sector can provide important technological solutions and a fresh perspective on design.
  - Accelerators and incubators.
    - Lower investment amounts but solid value-added services.

Funding Options (continued)

- Partnering with non-profits.
  - Patient advocacy and other not-for-profit organizations are increasingly involved in helping technologies/devices reach commercialization.
- Crowdfunding.
  - Risks associated with non-accredited investors.
  - Many states have issued legislation enabling equity crowdfunding, but Federal government still working through issues.
  - Negative signal to market?

Some Legal Basics

- Have a business structure in place, such as a corporation.
  - Alternative structures, such as LLCs, etc., possible, but corporate structure preferable.
  - Corporation should be formed in Delaware.
    - The Delaware General Corporation Law (the "DGCL") is a modern, current, and internationally recognized and copied corporation statute which is updated annually to take into account new business and court developments;
    - Delaware offers a well-developed body of case law interpreting the DGCL, which facilitates certainty in business planning;
    - The Delaware Court of Chancery is considered by many to be the nation's leading business court, where judges expert in business law matters deal with business issues in an impartial setting; and
    - Delaware offers an efficient and user-friendly Secretary of State's office permitting, among other things, prompt certification of filings of corporate documents.

Some (More) Legal Basics

- If you've closed friends/family round and/or angel round, be sure investment documents are in order.
  - Demonstrate compliance with unaccredited investor limits.
  - Reduce risk to later funder by demonstrating appropriate disclosure to early investors.
  - Angel round can help close the gap between seed investment and more substantive VC investment or other transactions.
- Founder/key person restrictions on securities transfers important.
- The number of authorized shares of Common Stock should be high enough to cover all outstanding shares of Common Stock, plus all shares of Common Stock that would be issued by converting certain other stock/options.

Some (More) Legal Basics

- Make sure your IP house is in order.
  - Keep careful records of applications, grants, etc.
  - If you license any IP from a third party, ensure that your use of such IP consistent with license grant.
  - Ensure that employees and consultants have appropriate IP language in their agreements (and make sure that they have agreements in the first instance).
  - Use NDAs when and where appropriate.
  - Careful documentation of IP can reduce concerns over third party infringement claims.
  - IP may be most significant driver in valuation, and in perception of whether your company can succeed.

Further Legal Basics

- Keep accurate books and records, with proper accounting processes from the beginning.
  - Unwinding opaque financials can harm the prospects of closing an investment.
  - Compliance with terms of grants.

Legal Concepts You Might Need to Know

- Common Stock vs. Preferred Stock
- Employee vs. Contractor
- Cumulative Voting
- Indemnification of Directors
- Bad Actors
- Transfers/Right of First Refusal
- Lock Up
- Tag-Along/Drag-Along
- Representations and Warranties

Arnall Golden Gregory LLP

Attorneys at Law

For more information, please contact:

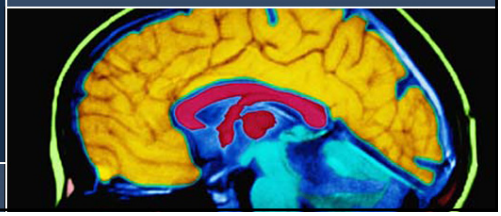
Michael E. Burke
Mike.Burke@AGG.com
202.677.4046

National Institute of Neurological Disorders and Stroke

NIH: Non-Dilutive Funding Opportunities

October 2015

Stephanie Fertig, MBA
Director, NINDS Small Business Programs
Office of Translational Research, NINDS
fertigs@ninds.nih.gov



National Institute of Neurological Disorders and Stroke

The Mission of NIH

…is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability.

The Mission of NINDS

…is to seek fundamental knowledge about the brain and nervous system and to use that knowledge to reduce the burden of neurological disease.

NIH National Institute of Neurological Disorders and Stroke

Disclaimer:

NINDS will be used as an example throughout. Individual NIH Institutes and Centers have different programs, guidelines and policies.

ALWAYS CONTACT PROGRAM STAFF WELL IN ADVANCE OF APPLYING.

NIH National Institute of Neurological Disorders and Stroke

Background: Neuromodulation

- **$3 Billion Dollar Industry** stimulation/recording from nervous system (2011 estimate)
- Example: Deep Brain Stimulation (DBS) for Parkinson's Disease
- Neuromodulation of End-Organ Systems Examples Recent Approvals:
  - Heart Failure: CVRx® Neo (Baroreceptors), BioControls CardioFit (Vagus), Cyberonics (Vagus)
  - Hypertension: CVRx® Neo (Baroreceptors), Renal Denervation (Medtronic, Boston Scientific St. Jude, Covidien, ReCor)
  - Obesity/Type II Diabetes: MetaCure Diamond (stomach muscles)

There are also lists of failed/stopped clinical trials

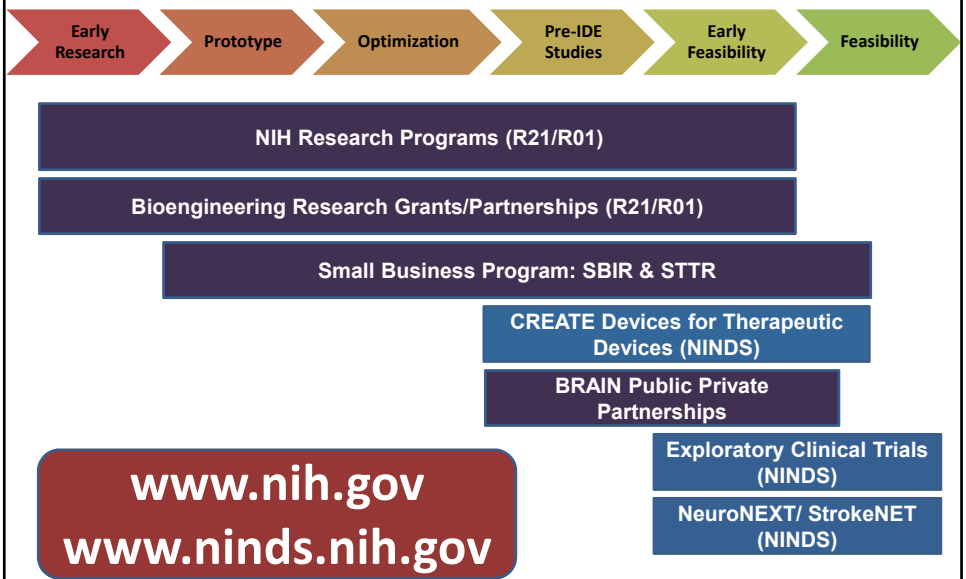
NIH National Institute of Neurological Disorders and Stroke

Treatments in Clinical Studies: Just the Vagus (Not Exhaustive)

- Heart Failure
- Hypertension
- Depression
- Anxiety
- Epilepsy
- Inflammation
- Stroke Rehab/Plasticity
- Tinnitus
- Diabetes
- Obesity
- Bronchioconstriction/Asthma
- Pain, Migraines, Cluster Headaches

NIH National Institute of Neurological Disorders and Stroke

NIH uses a Variety of Translational Approaches



NIH National Institute of Neurological Disorders and Stroke

NIH Small Business Programs

Small Business Innovation Research (SBIR)
Small Business Technology Transfer (STTR)

sbir.nih.gov

NIH National Institute of Neurological Disorders and Stroke

NIH Small Business Programs

Over $780M

Available for Small Businesses

- NINDS- Approximately $45M
- Broad scope
  - Therapeutics, diagnostics, and tools for research
  - May include bench research, translational research, and early stage clinical trials
  - ***Individual Institutes and Centers may Differ!***
- Waiver for some topics (e.g. animal and clinical studies) to support budgets over the hard cap

NIH National Institute of Neurological Disorders and Stroke

NINDS Small Business Clinical Studies

www.ninds.nih.gov/funding/small-business

- Clinical Research (e.g. diagnostics) are accepted through the general SBIR/STTR solicitations
- Do not accept SBIR/STTR Phase III clinical trials
- Phase I/II clinical trial or Device Feasibility/Pivotal trials
  - Not accepted through the general solicitation or as a Phase I SBIR/STTR
  - Accepted through specific program announcements
    - NINDS Exploratory Clinical Trials for Small Business
    - NINDS Direct to Phase II SBIR Grants to Support Exploratory Clinical Trials
    - StrokeNet and NeuroNEXT Clinical Trial Networks

NIH National Institute of Neurological Disorders and Stroke

SBIR/STTR Funding Opportunities for Devices

SBIR and STTR Funding Opportunities (90 Records - Sorted by Release Date)

Announcement Number	Issuing Organization	Other Participating Organizations	Release Date	Opening Date (SF424 Only)	Receipt Date(s)	Expiration Date	Activity Code(s)	Title
PA-15-354	NINDS	NCATS, NCI, NEI, NIAAA, NIDA, NIDCR, NINR	09/21/2015	Not Applicable	Standard Due Dates	09/06/2018	R43/R44,	SBIR Technology Transfer (R43/R44)
PA-15-336	NIDCR	NIBIB	08/20/2015	Not Applicable	Standard Due Dates	09/08/2018	R41/R42,	Imaging Diagnostics of Dental Diseases and Conditions (Caries, Periodontal Disease, Cracked Teeth, and Pulp Vitality) (R41/R42)
PA-15-335	NIDCR	NIBIB	08/20/2015	Not Applicable	Standard Due Dates	09/08/2018	R43/R44,	Imaging Diagnostics of Dental Diseases and Conditions (Caries, Periodontal Disease, Cracked Teeth, and Pulp Vitality) (R43/R44)
RFA-HG-15-033	NHGRI		08/17/2015	30 days prior to the application due date	October 27, 2015; July 14, 2016; June 15, 2017 , by 5:00 PM local time of applicant organization.	08/28/2017	R43/R44,	Novel Nucleic Acid Sequencing Technology Development (R43/R44)
RFA-HD-16-006	NICHD		08/12/2015	November 10, 2015	12/10/2015	12/11/2015	R41/R42,	Tools for Assessment and Improvement of Neurologic
RFA-HD-16-007	NICHD		08/12/2015	November 10, 2015	12/			

sbir.nih.gov

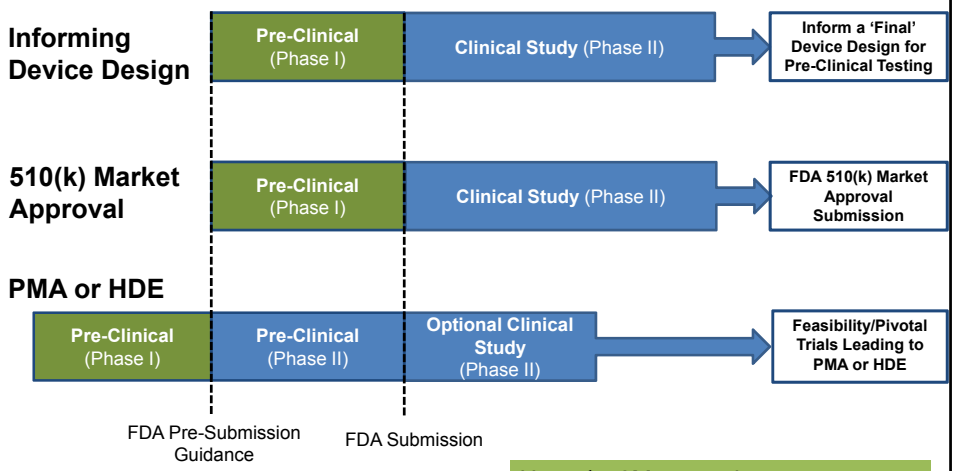
NIH National Institute of Neurological Disorders and Stroke

Cooperative Research to Enable and Advance Translational Enterprises (CREATE) for Therapeutic Devices

www.ninds.nih.gov/otr

NIH National Institute of Neurological Disorders and Stroke

NINDS CREATE Devices



Up to $7-8M per project over 5 years

NIH National Institute of Neurological Disorders and Stroke

NIH NSF FDA DARPA IARPA

Brain Research through Advancing Innovative Neurotechnologies (BRAIN)

HHMI HOWARD HUGHES MEDICAL INSTITUTE

SIMONS FOUNDATION

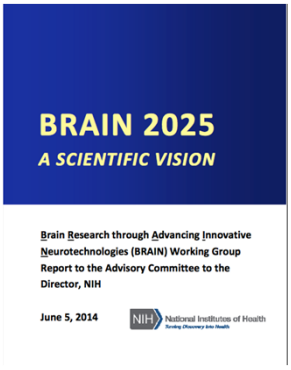
THE KAVLI FOUNDATION

ALLEN INSTITUTE for BRAIN SCIENCE Fueling Discovery

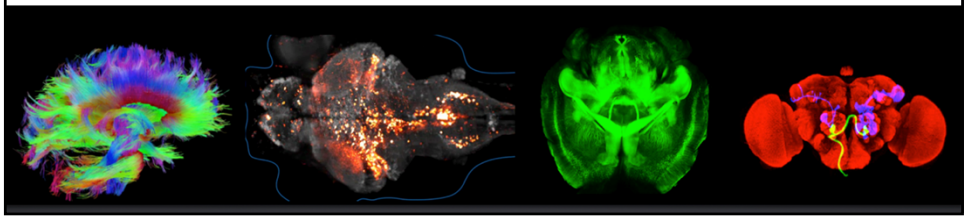
braininitiative.nih.gov

NIH National Institute of Neurological Disorders and Stroke

The BRAIN Initiative℠



- A focus on circuits and networks
- Measure the fluctuating electrical and chemical patterns within circuits
- Understand how all of this helps generate our unique thoughts and actions



The BRAIN Initiative: NIH Investment

Source
Blueprint for Neuroscience Research (BP)
Mental Health (NIMH)
Neurological Disorders and Stroke (NINDS)
Drug Abuse (NIDA)
Biomedical Imaging and Bioengineering (NIBIB)
Eye (NEI)
Office of Research in Women's Health (ORWH)
Behavioral and Social Sciences Research (OBSSR)

NCCIH
NEI
NIA
NIAAA
NIBIB
NICHD
NIDA
NIDCD
NIDCR
NIEHS
NIMH
NINDS
NINR
OBSSR

Nearly $85M in FY15

$25M was "new money" in FY 15 appropriation

FY16 Depends on Congressional Appropriation

BRAIN Initiative
Small Business Opportunities

PAR-15-090; PAR-15-091; PAR-15-121

Development, Optimization, and Validation of Novel Tools and Technologies for Neuroscience Research…

- for large scale recording/manipulation of neural activity
  - at or near cellular resolution,
  - at multiple spatial and/or temporal scales,
  - in any region and throughout the entire depth of the brain
- to facilitate the detailed analysis of complex circuits and provide insights into cellular interactions

Supports iterative refinement with the user community to increase incorporation into regular neuroscience practice

16

NIH National Institute of Neurological Disorders and Stroke

BRAIN Initiative
Human Research Opportunities

BRAIN Public-Private Partnership Program:
Industry Partnerships to Facilitate Early Access to Neuromodulation and Recording Devices for Human Clinical Studies

- Partnerships between clinical investigators and manufacturers of the latest-generation implantable devices for human clinical research
- Template Collaborative Research Agreements to streamline agreements between academic institutions and manufacturers

Applications Due: 11/18/2015	Pre-applications for Partnering with Commercial Manufacturers (**PAR-15-345**)
Applications Due: 4/26/2016	Full Proposals for Phased Translational-to-Clinical (**RFA-NS-16-009**) or Direct-to-Clinical (**RFA-NS-16-010**) Research

17

brininitiative.nih.gov/BRAIN_PPP/

NIH National Institute of Neurological Disorders and Stroke

BRAIN Initiative
Human Research Opportunities

Foundations of Non-Invasive Functional Human Brain Imaging and Recording - Bridging Scales and Modalities (RFA-MH-16-750)

Applications Due: 1/6/2016

- Studies to understand the biological basis and information content of contemporary non-invasive functional brain imaging techniques such as fMRI
- Bridge the gap between human neuroimaging signals and the underlying neural circuit events

Coming Soon: Research Opportunities using Invasive Recording/Stimulation in Humans (NOT-NS-15-002)

- Human research studies aimed at understanding brain function and disorders
- Take advantage of surgical settings using implantable stimulation and recording devices

Coming Soon: Non-Invasive Modulation in the Human Brain

18

brininitiative.nih.gov/funding_active.htm

NIH National Institute of Neurological Disorders and Stroke

Stimulating Peripheral Activity to Relieve Conditions (SPARC)

commonfund.nih.gov/sparc

NIH National Institute of Neurological Disorders and Stroke

SPARC Program Objective

Foster discovery and dissemination of the fundamental physiology and biological mechanisms underlying peripheral autonomic and sensory control of internal organ function and changes attributable to disease states and conditions.

Discoveries will enable development of:

- Next generation closed-loop neuromodulation therapies
- Investigation of approved devices for new indications
- Adoption of improved computational tools and modeling methods

20

NIH National Institute of Neurological Disorders and Stroke

SPARC Funding Opportunities

- No active funding opportunities at this time
  - Hiring Program Staff
  - **Expired** Opportunity: Exploratory Technologies to Understand Control of Organ Function by the Peripheral Nervous System
  - Several **Expired** Requests for Information
    - Data Informatics Needs and Challenges for Enabling SPARC
    - NIH-Industry Partnerships towards Clinical utility of Market-approved Devices to Support New Market Indications within SPARC
    - Research on Neural Control and Neuromodulation of Organ Function to Enable SPARC
    - Neuromodulation Technologies Needs and Challenges to Enable SPARC
- All NIH awards (including BRAIN and SPARC): projectreporter.nih.gov

commonfund.nih.gov/sparc

21

NIH National Institute of Neurological Disorders and Stroke

READ program announcements carefully
CONTACT us before applying

Stephanie Fertig: fertigs@ninds.nih.gov

@NINDS_SmallBiz

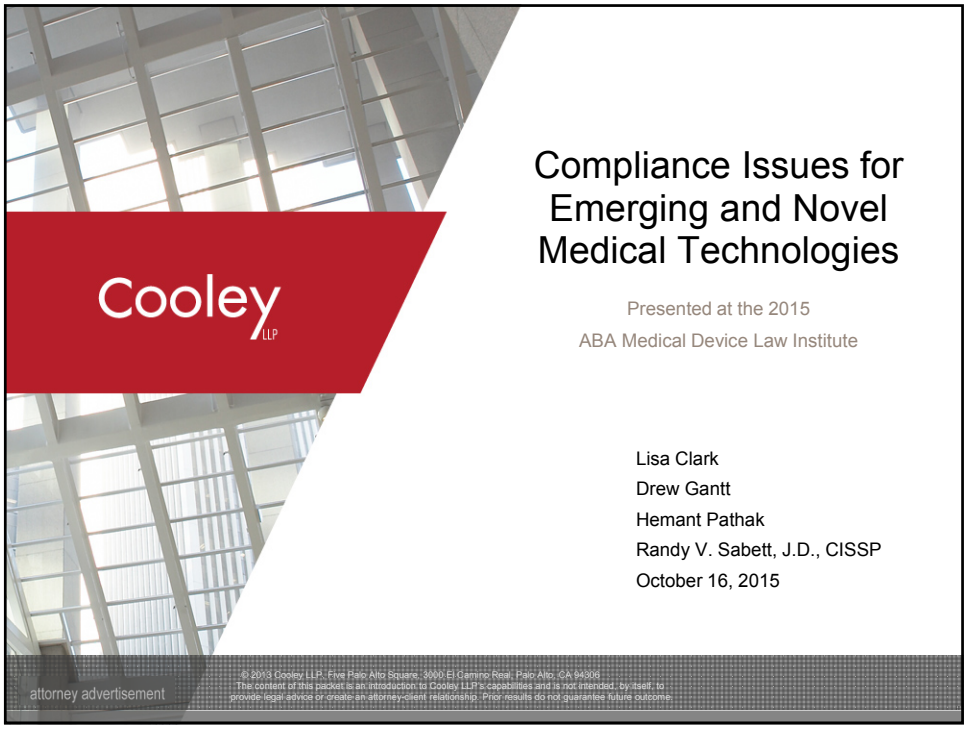
@NINDStranslate

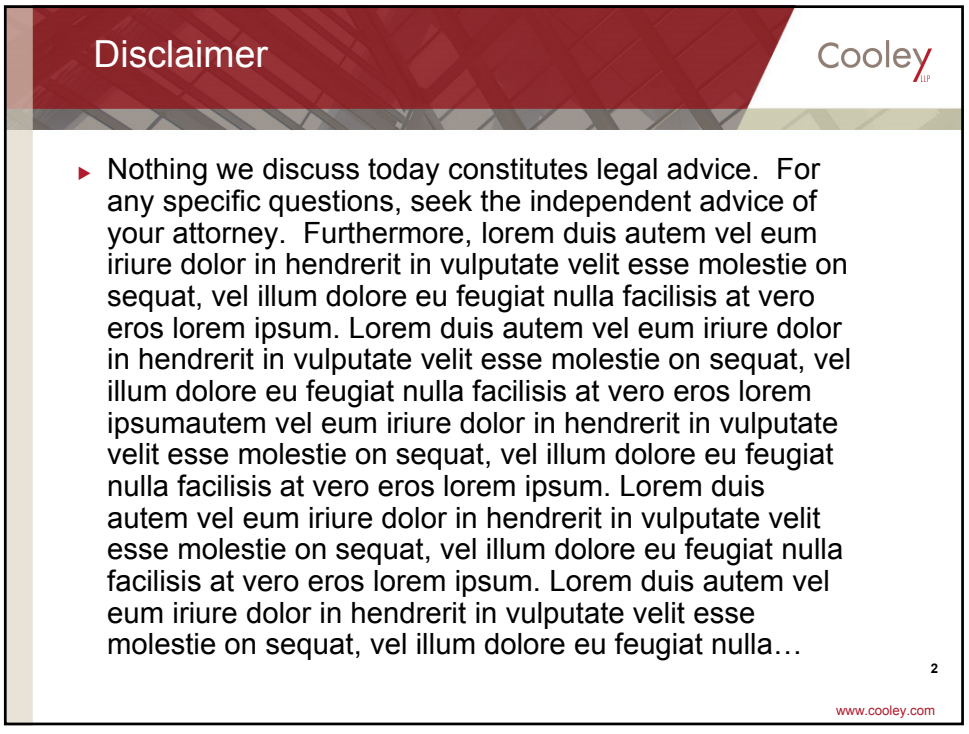
http://www.ninds.nih.gov/OTR

22

SECTION E

COMPLIANCE ISSUES FOR EMERGING AND NOVEL TECHNOLOGIES


Cooley LLP
Compliance Issues for Emerging and Novel Medical Technologies
Presented at the 2015
ABA Medical Device Law Institute
Lisa Clark
Drew Gantt
Hemant Pathak
Randy V. Sabett, J.D., CISSP
October 16, 2015
attorney advertisement
© 2013 Cooley LLP, Five Palo Alto Square, 3000 El Camino Real, Palo Alto, CA 94306
The content of this packet is an introduction to Cooley LLP's capabilities and is not intended, by itself, to provide legal advice or create an attorney-client relationship. Prior results do not guarantee future outcome.

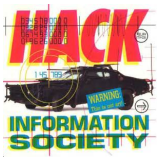

Disclaimer
Cooley LLP
Nothing we discuss today constitutes legal advice. For any specific questions, seek the independent advice of your attorney. Furthermore, lorem duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie on sequat, vel illum dolore eu feugiat nulla facilisis at vero eros lorem ipsum. Lorem duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie on sequat, vel illum dolore eu feugiat nulla facilisis at vero eros lorem ipsumautem vel eum iriure dolor in hendrerit in vulputate velit esse molestie on sequat, vel illum dolore eu feugiat nulla facilisis at vero eros lorem ipsum. Lorem duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie on sequat, vel illum dolore eu feugiat nulla facilisis at vero eros lorem ipsum. Lorem duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie on sequat, vel illum dolore eu feugiat nulla…
2
www.cooley.com

Med Devices, Cybersecurity, and Compliance

Why are we here today?

Cooley LLP

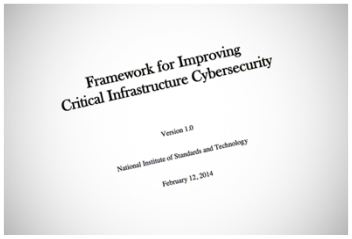
- Internet of Things / Internet of Everything / [The next big thing…] are poised to explode the connectivity of our world
- Devices generally have been connected for a long time but at a local or unseen level (as just two examples, think about the recent car hacking incidents and attacks on ATMs)
  - Med devices fall into this category
  - Not something new to the public (recall Dick Cheney's concerns about outside access to his pacemaker by terrorists)
  - Death of Barnaby Jack (who once told Reuters that "he could kill a man from 30 feet away by attacking an implanted heart device") adds to the intrigue
- FDA has been addressing the issue and has released some recent guidance based on the NIST cybersecurity framework



Levelset: The NIST Framework

Cooley LLP

- Focus on critical infrastructure.
- Purports to be agnostic..
- It's a framework, not a standard.
- IT'S A FRAMEWORK, NOT A STANDARD.



Remarks on its release:

- **Rebecca Blank (Commerce)**: "Administration is stepping up to the plate" and "cybersecurity cannot be addressed by government alone."
- **Mike Daniel (EOP)**: Approach based on "information sharing, privacy, and a framework of standards." Also, EO "is just a down payment until legislation passes."
- **General Alexander (NSA)**: Although the Framework addresses hard challenges, "we need legislation to which everyone can agree" and that will "liability concerns."
- **Pat Gallagher (NIST)**: Distinguished between standards and norms as a way of illustrating how the Framework will be developed.

Again…It's Only a Framework

Cooley LLP

- Pulls together concepts from threat analysis, risk management, and operational security to derive an approach built around:
  - **A set of core elements** comprising functions, categories, subcategories and references.
  - **Framework tiers** that reflect how the core elements are implemented.
  - **Profiles** that allow tracking between the current state of an organization's cybersecurity efforts and its target state.
- Ultimately, it's only 12 pages long…OK, so I'm playing a bit fast and loose on that one.

Selected Timeline

2008 –Commission on Cybersecurity for the 44th Presidency.

May 8, 2009 – Melissa Hathaway and the 60-day review.

May 29, 2009 – "America's economic prosperity in the 21st century will depend on cybersecurity."

President Obama, Remarks on Securing Our Cyber Infrastructure.

Hmmmm….what exactly happened here?

February 2013 – Executive Order 13636.

August 2013 – Discussion draft released.

October 2013 – Preliminary Cybersecurity Framework released.

December 2013 – End of 90-day comment period.

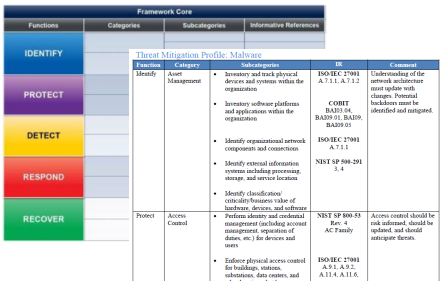
Feb. 12, 2014 – Release of final Cybersecurity Framework.

2015 – Adoption by several agencies

Core Elements

Cooley LLP

- "Present key cybersecurity outcomes identified by industry as **helpful in managing cybersecurity risk**."
- Those activities map to existing standards and guidelines.
- The core elements allow for common discussions about cybersecurity and risk management across a range of stakeholders.
- Distributed across the core functions of **Identify, Protect, Detect, Respond and Recover**, the core elements comprise categories of cybersecurity activities that are further broken down into subcategories.



Important point– The Framework makes very clear that the it **"complements, and does not replace, an organization's existing risk management process and cybersecurity program."**

Implementation Tiers and Profiles

Cooley LLP

- **Implementation tiers**
  - Implementation tiers "reflect how an organization implements the Framework Core functions and categories and manages its risk."
  - Range from PARTIAL (no formal process), to RISK-ASSESSMENT ("threat-aware risk management process), to REPEATABLE (regularly utilizes/updates its process), to ADAPTIVE (utilizes predictive mechanisms).
- **Profiles**
  - Profiles allow for a **gap analysis** (which is not a new concept).
  - The big difference is how the Framework Profile concept integrates with rest of the Framework.
    - An entity's current Profile represents the present cybersecurity state of that entity, while the target Profile represents the goal or end state.
    - Most importantly, the Profiles align with the "business requirements, risk tolerance and resources of the organization."

Some History From The FDA…

Cooley LLP

- Some history from the FDA:
  - **2005**: "only have two reports of incidents related to a cybersecurity threat or cybersecurity vulnerability"
  - **2010**: VA Cath Lab had temporary closure due to malware infecting computers that are used for interventional cardiac procedures
  - **2011**: researcher showed feasibility of hacking implantable insulin pump
  - **2013**: two researchers provided a "very very significant package" of vulnerabilities related to med devices with hardcoded passwords
  - **2015**: "FDA has no knowledge of there ever having been an intentional exploit that as carried out that resulted in patient harm."
  - **2015**: Researchers have provided to FDA device vulnerabilities that are "too numerous to list"

> "There is no such thing as a threat-proof medical device…It is important for medical device manufacturers to remain vigilant about cybersecurity and to appropriately protect patients from those risks."
>
> - Suzanne Schwartz, M.D., MBA, director of emergency preparedness/operations and medical countermeasures

Some Vulnerabilities of Which FDA is Aware

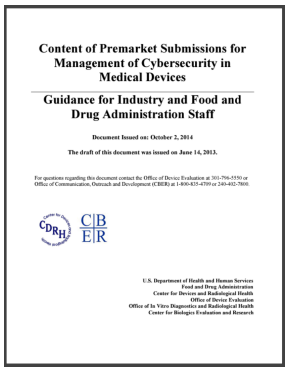
Cooley LLP

- Lack or slow adoption of software updates and patches to medical devices and networks
- Failure to address vulnerabilities in older medical device models
- Malware infection and disabling of networked medical devices
- Targeting of mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices
- Distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel)
- Vulnerabilities in third party software, such as plain-text or no authentication, hard-coded passwords, service accounts described in non-confidential service manuals, and "buggy" coding

FDA Guidance on Med Device Cybersecurity

Cooley LLP

- *Guidance* on cybersecurity for:
  - "identifying issues…that manufacturers should consider **in the design and development** of their medical devices as well as in preparing premarket submissions for those devices" (emphasis added)
  - reducing risk based on **intentional or unintentional compromise** of devices
- Applies to premarket submissions for devices containing software or programmable logic, as well as "software that is a medical device"
- 'Cybersecurity': preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient"



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

CDRH CBER

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

FDA Guidance on Med Device Cybersecurity (cont'd)

Cooley LLP

- FDA recommends device manufacturers consider **Identify, Protect, Detect, Respond, and Recover** (look familiar?)
- Identify considerations include:
  - intended use of medical device, presence of electronic data interfaces, intended use environment, vulnerabilities present, likelihood vulnerabilities will be exploited (intentionally or unintentionally), and the probable risk of patient harm due to a cybersecurity breach
- Protect considerations include:
  - use authentication to limit access to med devices
  - ensure trusted content (e.g., properly authenticated code)
- Detect, Respond, and Recover
  - all addressed together by FDA
  - implement detection technology and educate users
  - have a response plan and recovery process

Potential liability for cybersecurity vulnerabilities

Cooley LLP

Liability Theories

- Product liability
  - Defective design
  - Defective manufacture
  - Defective marketing
  - Failure to warn
- Contract liability
- Statutory liability
  - DMCA
  - CFAA

Stakeholders

- Manufacturer
- Supply chain
- Software/firmware author
- Hospital/facility
- Caregiver
- Consumer
- Researcher
- Hacker

The Wrap-Up

Cooley LLP

1. **Vulnerability discovery increasing exponentially**
2. **Researchers revealing new and innovative hacks**
3. **Actual cases do exist and also on the rise**
4. **No actual harm (yet) from deliberate act**
5. **NIST framework gaining acceptance**
   1. **Identify, Detect, Protect, Respond, Recover**
   2. **Adopted by FDA in latest med device guidance**
6. **Cyber should be part of design process from the beginning, not an afterthought**

Contact info

Lisa Clark
Duane Morris LLP
(215) 979-1833 (o)
lwclark@duanemorris.com

Drew Gantt
Cooley LLP
202.728.7090 (o)
dgantt@cooley.com

Hemant Pathak
Assistant General Counsel
Microsoft

Randy V. Sabett, J.D., CISSP
Cooley LLP
202.728.7090 (o)
rsabett@cooley.com

SECTION F

EVOLVING HIPAA AND PRIVACY ISSUES FOR THE MEDICAL DEVICE INDUSTRY

EVOLVING HIPAA AND PRIVACY ISSUES FOR MEDICAL DEVICE INDUSTRY

Matthew Fisher, Esq.; Mirick O'Connell
Clinton Mikel, Esq.; The Health Law Partners
Gregory Noonan, Esq; Collora LLP
Mauricio Paez, Esq.; Jones Day
Philip Brewster; Esq.; Brewster Law Firm LLC

What is HIPAA?

- The Health Insurance Portability and Accountability Act ("HIPAA") of 1996
  - Addresses numerous healthcare issues
  - Was signed into law by President Clinton on August 21, 1996
- Privacy and Security Rules under HIPAA are designed to protect sensitive information known as "Protected Health Information" ("PHI")
- The Health Information Technology for Economic and Clinical Health Act of 2009 expanded HIPAA's coverage to include electronic information and require notification of breaches
- Also covers other issues such as billing and insurance provisions, but those will not be covered here

HIPAA: Who is Subject?

- Covered Entities
  - Health Care Providers (meeting certain conditions)
  - Health Insurers
  - Health Care Clearinghouses
- Business Associates
  - Any entity that assists with or performs functions for or on behalf of a covered entity for any activity regulated by HIPAA
  - Very broad
- Subcontractors of Business Associates

HIPAA: What does it Cover?

- "Protected Health Information" or "PHI"
- Term of art defined by statute and regulations
- If not PHI, then not covered by HIPAA

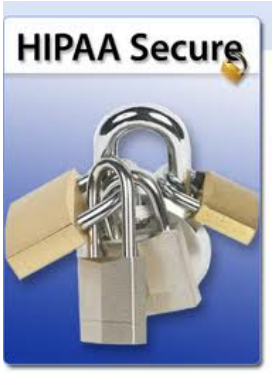
- Coverage driven by context

HIPAA: Privacy Rule

- General Purpose – regulates "use" and "disclosure" of PHI by "covered entities," "business associates," and subcontractors
  - Allows for certain, limited uses and disclosures without requiring authorization
  - Others require notice to and/or authorization from the patient
- Imposes numerous compliance requirements on entities (*e.g.* tracking, reporting, training)

HIPAA: Security Rule

- General purpose – creates standard security measures for the protection of PHI that is created, received, used or maintained by covered entity
- Includes various technical, administrative, and physical requirements and specifications
- A primary concern with increasing number of threats to medical and electronic information



HIPAA: Breach Notification Rule

- General purpose - requires notification if a "breach" of PHI occurs
  - Applies to a breach by *any entity* handling PHI
  - Final rule claimed to create an objective standard, but still has subjective elements
  - Breach presumed to have occurred
  - Breached entity must prove why notification is not needed

Why Care About HIPAA?

- How do HIPAA and medical devices companies interact?
  - Depends on what medical device does, who will use it, where PHI may go, what PHI will be stored, and more
- Typically, medical device company be a business associate
  - Device collects PHI
  - Stores and/or transmits somewhere – to data storage, health information exchange, provider, or others
  - Means medical device company viewed as acting for or on behalf of a covered entity
- BUT, can be health care provider (or covered entity) too
  - Does medical device company bill for, furnish, or provide "health care?"
- Compliance gains trust of clients
  - Compliance expected
  - Sets baseline for standards in operations

How Comply with HIPAA

- How can a medical device company comply with HIPAA?
  - First Step – review terms of business associate agreement
  - Second Step – perform risk analysis
  - Third Step – prepare policies and procedures
  - Fourth Step – implement policies and procedures
  - Fifth Step – continually monitor and refine policies and procedures

HIPAA Compliance – First Step

- Business Associate Agreement
  - Terms driven by HIPAA regulations
  - Requirements found in both the Privacy Rule and the Security Rule
  - Generally, business associates need to comply with all of the Security Rule and select pieces of the Privacy Rule
  - What else?
    - Look at terms to understand what is stated
    - Can impose faster response times than may get directly under HIPAA regulations
    - See if there are requirements above and beyond the HIPAA regulations

HIPAA Compliance – Second Step

- Perform a RISK ANALYSIS
- Essential element and first step in complying with the Security Rule
- Means to “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information.” (45 CFR 164.308(a)(1)(ii)(A))
- Comprehensive overview that enables entity to assess what needs to be done

HIPAA Compliance – Third Step

- For Security Rule
  - Use results from risk analysis
  - Go through technical, administrative, and physical components
  - Implement all required and analyze addressable elements
- For Privacy Rule
  - If only in a BA capacity, then Business Associate Agreement provides a guide
  - Will not need to implement all aspects of Privacy Rule
- Do not utilize off the shelf policies and procedures
- Seek assistance in developing and/or reviewing

HIPAA Compliance – Fourth Step

- Now that you have policies and procedures, have to implement
- Means educating, training, and generally getting people aware
- If no one in the organization understands what is required, cannot expect compliance
- Education includes explaining what HIPAA is and does
- Training should occur with implementation (or new hire) and then recur annually

Image from www.hipaasecurenow.com

HIPAA Compliance – Fifth Step

- Monitor, modify, listen, and evolve
- Compliance is not static, must continually adapt
- Have to monitor activities to find non-compliance or other issues
- Modify when new issues come up
- Listen to employees or others interacting with the policies and procedures
- Make HIPAA compliance a living, breathing plan
  - Everyone needs to buy in and play a role

Is Medical Device Company Always a BA?

- Do not forget: possible for medical device company to be a health care provider
  - Means not necessarily in business associate category
- How does it happen?
  - If provides health care as defined by HIPAA, then will be a health care provider
  - Can occur if counsel physician on how to use the device, or assist in adjusting or using the device, among other ways
  - If the device company will bill directly, can receive PHI
- What are implications of being a health care provider?
  - May not need a Business Associate Agreement
  - Protected Health Information can be shared in different ways
- Some potential to also be a covered entity
  - If a covered entity, then need to comply with all aspects of the Privacy Rule

What Does HIPAA Mean for the Actual Device?

- How is a medical device made compliant?
  - Remember, entities are compliant, not devices
  - By following steps identified above, entity can be compliant
  - Having device meet security standards and have appropriate security controls helps the entity comply
- Pay most attention to security requirements
  - What standards use? – NIST, FDA, more
  - Consider where PHI going
    - Physician, HIE, other
  - Gaining attention from hacking reports

Summary

- Never forget, entities are compliant, not devices
- Determine role being played, i.e. business associate, health care provider, or maybe covered entity
- No matter what, develop policies and procedures
- Put significant focus on Security

Image from www.contactcenterworld.com

SECTION G

PRACTICAL CYBER SECURITY FOR THE DEVICE INDUSTRY

DuaneMorris

Practical Cyber Security for the Medical Device Industry

October 16, 2015

Moderated by Michael E. Clark

2nd Annual ABA-FDLI-MDMA MEDICAL DEVICE CONFERENCE
October 15-16, 2015
Washington, DC 20036

ABA American Bar Association Health Law Section

MDMA Medical Device Manufacturers Association *Innovation Today for Better Health Care Tomorrow™*

FDLI

Legal Landscape – Federal Regulation

DuaneMorris

Patchwork of Legislative and Administrative Standards

- Federal Trade Commission Act ("FTC Act")
- Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Health Information Technology for Economic and Clinical Health Act ("HITECH Act")
- Gramm-Leach-Bliley Act ("GLBA")
- Federal Americans with Disabilities Act ("ADA")
- Children's Online Privacy Protection Act ("COPPA")
- Fair Credit Reporting Act ("FCRA") and Fair and Accurate Credit Transactions Act ("FACTA"), Electronic Communications Privacy Act (Stored Communications Act and Wiretap Act), and Telephone Consumer Protection Act.
- Video Privacy Protection Act ("VPPA")
- National Institute of Standards and Technology ("NIST")

DuaneMorris

Patchwork of legislative and administrative standards (cont.)

- SEC Requirements:
  - **Division of Corporation Finance Disclosure Guidance: Topic No. 2 Cybersecurity** (October 13, 2011) – guidelines for public corporations who suffer cyber attacks or data breaches
  - **SEC Sweep Letters** (2014) – the SEC asking for information about firms' cybersecurity practices
  - **Cybersecurity Roundtable** (March 26, 2014) – SEC held roundtable discussion
  - **Rule 13(a)-15(f) of the Exchange Act (ICFR)** – Adopting release effective August 14, 2003
  - **SEC's Cybersecurity Examination Sweep Summary** (February 3, 2015) – released findings and industry practices report

DuaneMorris

Patchwork of legislative and administrative standards (cont'd)

- New Legislation: Cyber Intelligence Sharing and Protection Act ("CISPA") (reintroduced in the House in January 2015) H.R. 624 (113th Congress)
- Any company can "use cybersecurity systems … to protect the rights and property" of the company, then share that information with third parties, including the government, so long as it is for "cybersecurity purposes."
- If enacted, could allow the government to hold critical infrastructure businesses accountable for failing to make measurable improvements.

Legal Landscape – State Regulation

DuaneMorris

State Legislation

47 states, District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches:

- **Who Must Comply with the Law?**
  - Businesses, data/ information brokers, gov't entities
- **Definitions of "personal information"**
  - Name combined with SSN, driver's license or state ID, account numbers
- **What constitutes a breach?**
  - Unauthorized acquisition of data
- **Requirements for notice**
  - Timing or method of notice
  - Who must be notified?

Legal Landscape – Government Enforcement Actions

DuaneMorris

Federal Trade Commission Enforcement

- **Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a)**, prohibits "unfair or deceptive acts or practices in or affecting commerce"
- More than 30 enforcement actions have been brought by the FTC since May 1, 2011. The FTC has brought more than 50 actions in all since 2000
- FTC's Health Breach Notification Rule

DuaneMorris

FTC Launches Investigative Arm to Tackle Technology

- FTC is expanding a special unit dedicated to fraud detection and consumer protection: *The Office of Technology Research and Investigation* (the "OTRI")
- "*The OTRI is the successor to the [Mobile Technology Unit], and will build upon their great work by tackling an even broader array of investigative research on technology issues involving all facets of the FTC's consumer protection mission, including privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, big data, and the Internet of Things.*" – Ashkan Soltani, FTC's Chief Technologist

DuaneMorris

President Obama Addresses Cybersecurity Issues, Signs Executive Order at Stanford University

- "Just like we do with terrorist threats, we're going to have a single entity that's analyzing and integrating and quickly sharing intelligence about cyber threats across government so we can act on all those threats even faster." – President Obama, February 13, 2015
- Obama administration is working toward establishing a single national standard that will ensure that Americans are notified within 30 days if their information has been stolen, and it has also proposed the Student Digital Privacy Act
- In the same week, the White House also announced the creation of its Cyber Threat Intelligence Integration Center
- President signed an executive order which calls for a common set of standards around protecting privacy and civil liberties

DuaneMorris

President Obama Signs Executive Order to Block Property of Those Engaging in Malicious Cyber-Enabled Activities

- President Obama signed an Executive Order on April 1, 2015, blocking the property of designated or to-be-designated individuals engaging in malicious cyber-enabled activities that constitute an unusual and extraordinary threat to the United States
- The Executive Order contains traditional blocking language, including the prohibition relating to donations and other assistance to "blocked persons"

DuaneMorris

Data Security and Breach Notification Act of 2015

- On March 25, 2015, the *United States House of Representative, Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade* approved draft legislation which would replace state data breach notification laws with a national standard

DuaneMorris

Data Security and Breach Notification Act of 2015 (cont'd)

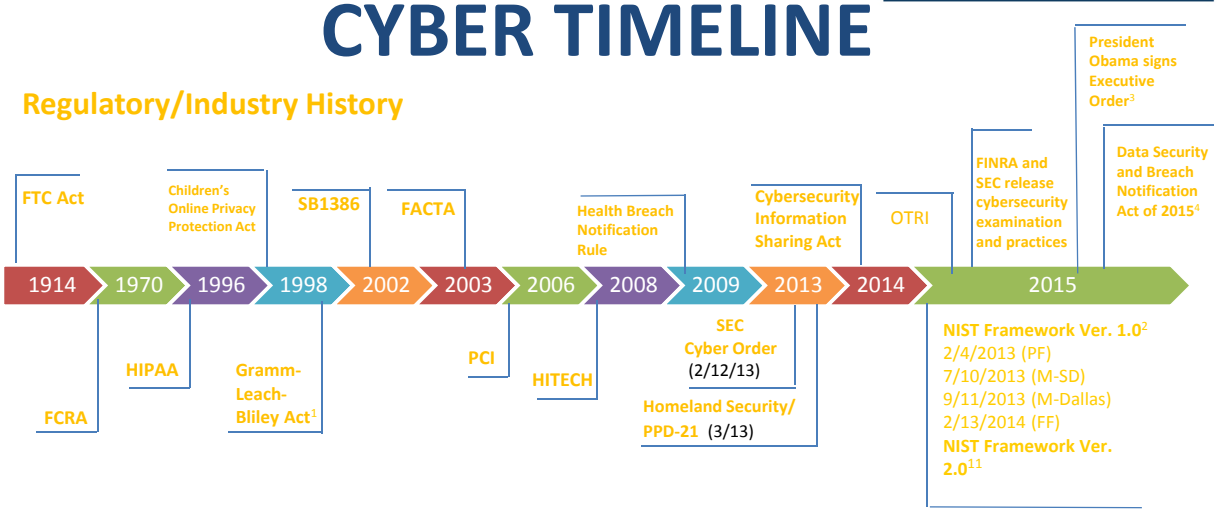
The draft legislation contains several key provisions:

1. Companies would be required to implement and maintain reasonable security measures and practices to protect and secure personal information
2. The definition of personal information is more expansive than most state breach notification laws, including home address, telephone number, mother's maiden name, and date of birth as data elements
3. Companies are not required to provide notice if there is no reasonable risk of identity theft, economic loss, economic harm, or financial harm
4. Companies would be required to provide notice to affected individuals within 30 days after discovery of a breach
5. The law would preempt all state data breach notification laws
6. Enforcement would be by the Federal Trade Commission (FTC) or state attorneys general
7. No private right of action would be permitted

DuaneMorris

CYBER TIMELINE

Regulatory/Industry History

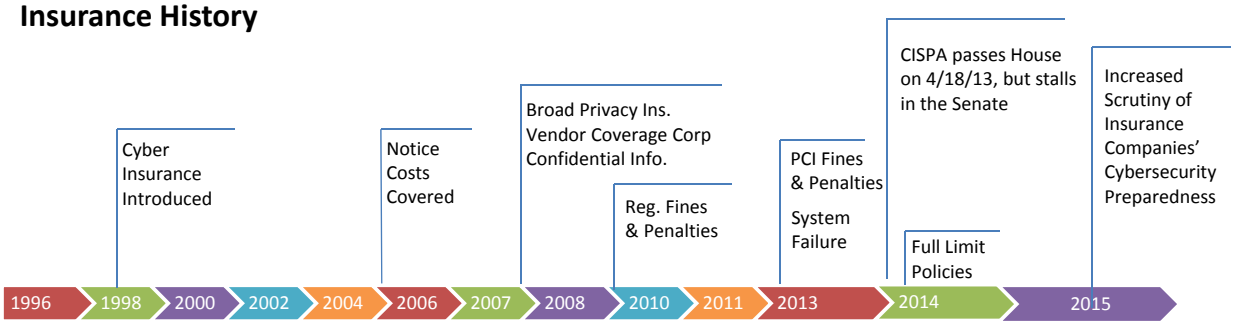


[1] GLB requires private financial information to be properly protected
[2] Framework for Improving Critical Infrastructure Cybersecurity
[3] NIST will continue to serve as convener and coordinator at least through version 2.0 of Framework
[4] President Obama addressed cybersecurity issues and signed executive order at Stanford University in February 2015
[5] On March 25, 2015, the United States House of Representative, Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade approved draft legislation which would replace state data breach notification laws with a national standard

DuaneMorris

CYBER TIMELINE

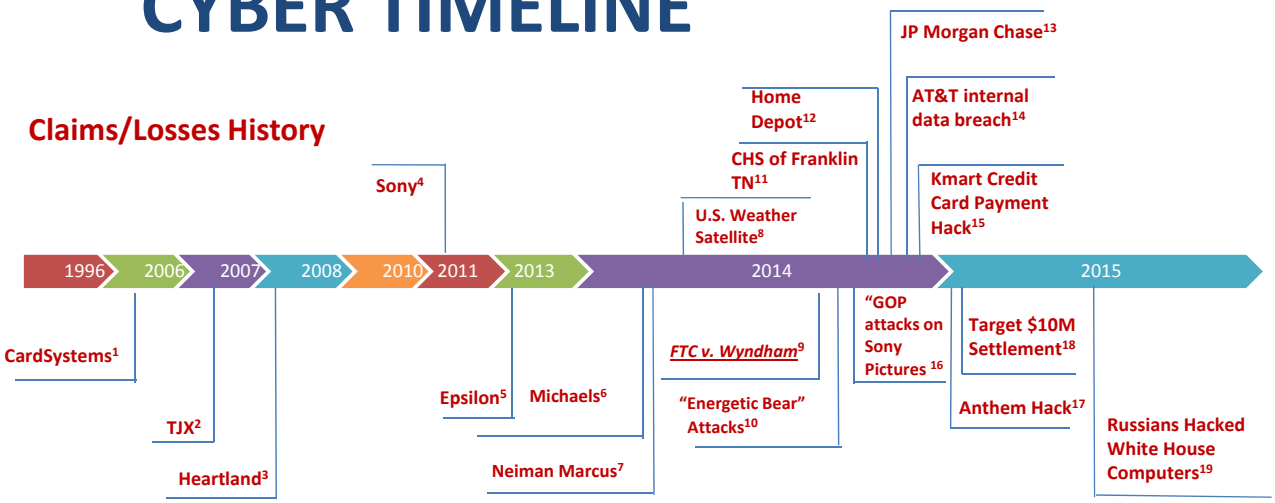
Insurance History



DuaneMorris

CYBER TIMELINE

Claims/Losses History



1. Resulted in millions of dollars in fraudulent purchase.
2. $45 million credit and debit cards were stolen (2007).
3. $140MM in fines and settlements (2007).
4. Sony PlayStation/BMG's website breaches (cleanup $171MM) (2010).
5. Data breach ("spear phishing") involving names of customers and email addresses/affected at least 50 companies (2011).
6. Michaels Stores disclosed on April 18, 2014.
7. NM was hacked from July to December 2013.
8. China hacks into U.S. weather satellite data include forecasts.
9. District court grants interlocutory appeal on June 23, 2014.
10. Russian hackers attack U.S. and European energy companies, and be capable of disrupting power supplies.
11. Hackers stole 4.5 million patient records by breaking into the company's network through a hole in the network created by Heartbleed.
12. Home Depot's breach is expected to cost the company $62 million (53 million email addresses and 56 million credit card accounts were stolen in the hack).
13. October 2, 2014 securities filing disclosed that a cyberattack compromised data for 76 million households and 7 million businesses.
14. Employee gained access to 1600 customer's personal data records.
15. Initial investigation suggests the cyber-thieves stole credit and debit card numbers – numbers undetermined.
16. Guardians of Peace" repeatedly attacks SPE which causes movie chains to cancel Sony films.
17. Anthem Health Insurance hack exposes data of 80 million.
18. Target to settle massive data breach for $10 million from the 2013 hack.
19. The hackers gained access to sensitive information from the White House.

Homeland Security

DuaneMorris

February 12, 2013

Chemical Sector
The Department of Homeland Security

Commercial Facilities Sector
The Department of Homeland Security

Communications Sector
The Department of Homeland Security

Critical Manufacturing Sector
The Department of Homeland Security

Dams Sector
The Department of Homeland Security

Defense Industrial Base Sector
The Department of Defense

Homeland Security

DuaneMorris

Emergency Services Sector
The Department of Homeland Security

Energy Sector
The Department of Energy

Financial Services Sector
The Department of Treasury

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services

Government Facilities Sector
The Department of Homeland Security and the General Services Administration

Healthcare and Public Health Sector
The Department of Health and Human Services

Homeland Security

DuaneMorris

Information Technology Sector
The Department of Homeland Security

Nuclear Reactors, Materials, and Waste Sector
The Department of Homeland Security

Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation

Water and Wastewater Systems Sector
The Environmental Protection Agency

DuaneMorris

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

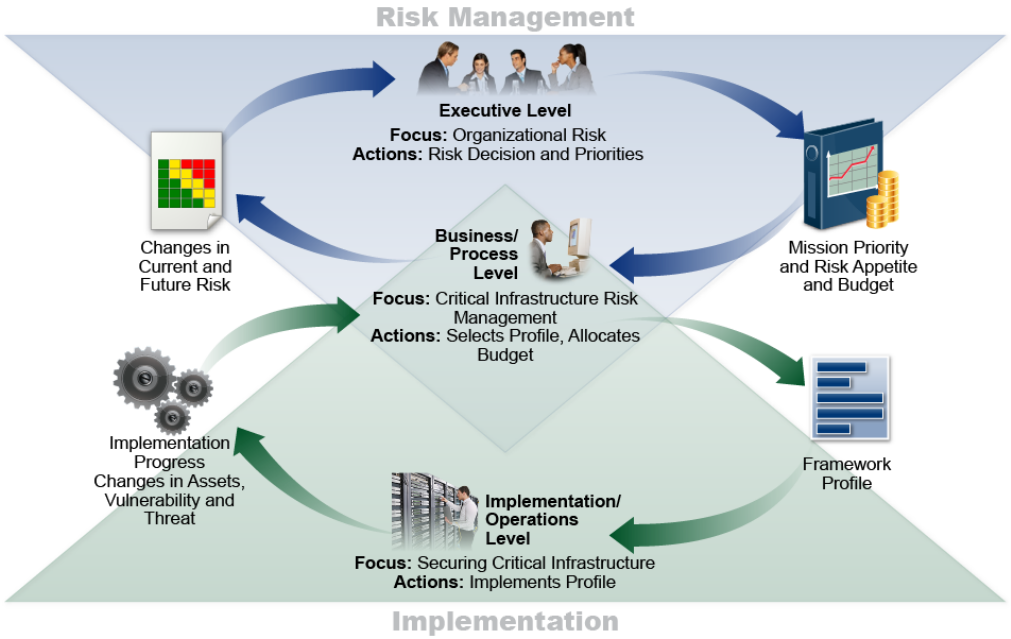
DuaneMorris

Framework Implementation Tiers

Tier	Risk Management Process	Integrated Risk Management Program	External Participation
Tier 1: Partial	Informal risk practices, reactive, ad hoc risk approach	Limited institutional awareness. Risk management in place but irregular	Lacks processes to coordinate collaborate
Tier 2: Risk Informed	Approved risk mgmt. practices but not organization-wide. Priorities informed by stakeholder goals and corporate risk decisions	Organization has cybersecurity risk awareness but not yet an institutionalized approach	Organization has not formalized capabilities to interact and share information
Tier 3: Repeatable	Risk mgmt practices formally approved, expressed as policy, regularly updated	Organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed	Org. understands dependencies and partners, receives info that enables collaboration and risk-based response decisions
Tier 4: Adaptive	Adapts based on lessons learned. Continuous improvement, timely response	Organizational risk approach with situational awareness integrated into culture	Active sharing with partners to proactively learn and benefit the community

Coordination of Framework Implementation

DuaneMorris



The image above describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

DuaneMorris

Healthcare

- The Durkheim Project, funded by the U.S. Department of Veteran Affairs, analyzes social-media behavior to detect early signs of suicidal thoughts among veterans
- Machine-learning algorithms in the gaming industry to detect early signs of gambling addiction
- Apple HealthKit - 23 health and wellness apps that track activity, diet, and sleep
- Biometric Identification - Identifies patient by the vein pattern in hand – ensures the right patient receives the right treatment (Baptist Health Hospital in Florida and UC San Diego)




DuaneMorris

PatientSecure
Biometric Identification Systems

Factors that affect pricing:

- ✓ the # and bed size of acute-care hospitals
- ✓ the # of ambulatory locations
- ✓ the # of HIS/EMR registration workflows that require interfacing
- ✓ the # of Palm Vein Scanning devices needed to cover all points of patient registration and mobile carts in the ED
- ✓ the # of Kiosks and functionality required, etc.

DuaneMorris

Apple Watch raises FTC concerns related to privacy

- FTC meets with Apple regarding health data gathered by Apple Watch and other Apple gadgets to ensure that data will not be shared with third-party without user consent

DuaneMorris

"You're going to be hacked."

"Have a plan."

- Joseph Demarest, assistant director of the FBI's cyberdivision.

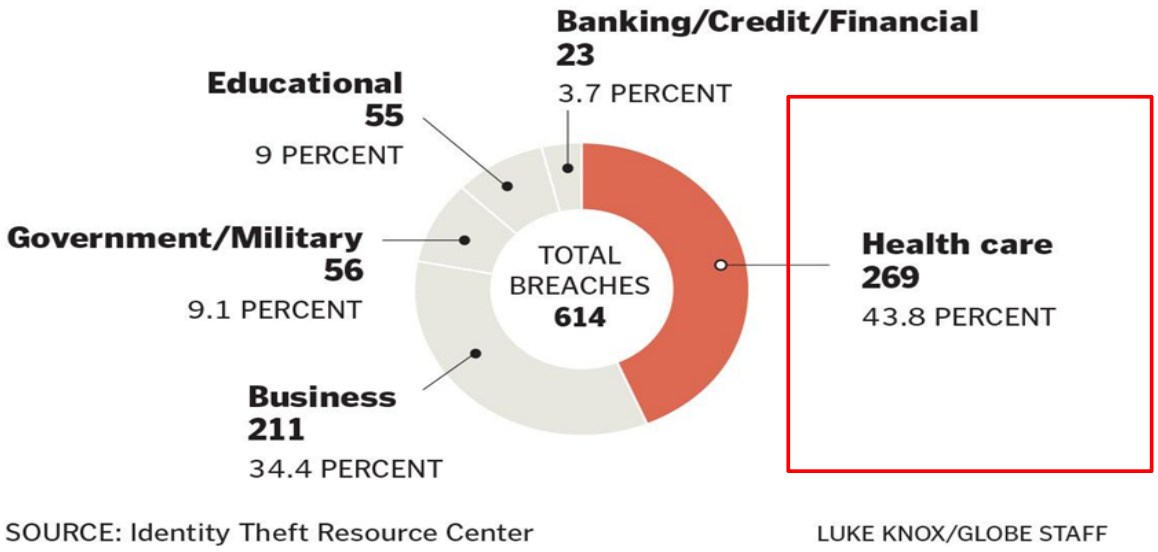
DuaneMorris

Cyber-Insurers Will Demand Better InfoSec

Cyber-insurance companies are sending in assessors to get a better look at a potential client's security risks

DuaneMorris

Data breaches by industry, 2013



Source: ***Hackers threaten health care industry's patient records*****, Boston Globe (Sept. 6, 2014)**

DuaneMorris

Stolen Health Data of High Value of Cybercriminals

- **Medical data more valuable than credit card data**. Theft of medical records is often not immediately identified by patients or their providers, giving cybercriminals sometimes years to use such data, making medical data more valuable than credit card data.
- Cybercriminals target medical records for patients' names, birth dates, policy numbers, diagnosis codes and billing information.
- Data is often used to forge ID cards to buy medical equipment or prescription drugs that can be resold.

DuaneMorris

Stolen Health Data: High Value of Cybercriminals

- Healthcare records can be $10 per record (compared to $1 per credit card record in Russian markets)
- In 2013, a patient learned that his medical records had been compromised after he started receiving bills related to a heart procedure he had not undergone. His medical information was also used to buy a mobility scooter and several pieces of medical equipment, totaling tens of thousand of dollars in fraudulent charges
- Target inferred that a teenage customer was pregnant and, by mailing her coupons intended to be useful, unintentionally disclosed this fact to her father

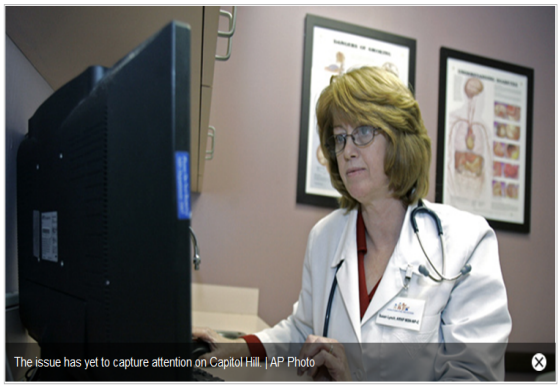
How Vulnerable is the Health Care Industry?

DuaneMorris

POLITICO Pro Learn more

Electronic health records ripe for theft

Tweet 525 Share 272 Share 65 299



The issue has yet to capture attention on Capitol Hill. | AP Photo

By DAVID PITTMAN | 7/13/14 9:56 PM EDT

America's medical records systems are flirting with disaster, say the experts who monitor crime in cyberspace. A hack that exposes the medical and financial records of hundreds of thousands of patients is coming, they say — it's only a matter of when.

As health data become increasingly digital and the use of electronic health records booms, thieves see patient records in a vulnerable health care system as attractive bait, according to experts interviewed by POLITICO. On the black market, a full identity profile contained in a single record can bring as much as $500.

"The high value of health information makes it attractive to hackers. . . . The record contains financial records, personal information, medical history, family contacts — enough information to build a full identity."

www.politico.com/story/2014/07/electronic-health-records-theft-108856.html#ixzz3ESN9YOhQ

Medical Devices & Hospitals

DuaneMorris

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION MA

THREAT LEVEL

It's Insanely Easy to Hack Hospital Equipment

BY KIM ZETTER 04.25.14 | 6:30 AM | PERMALINK

Share 0 +1 465 Share 1,374 Pin it 1

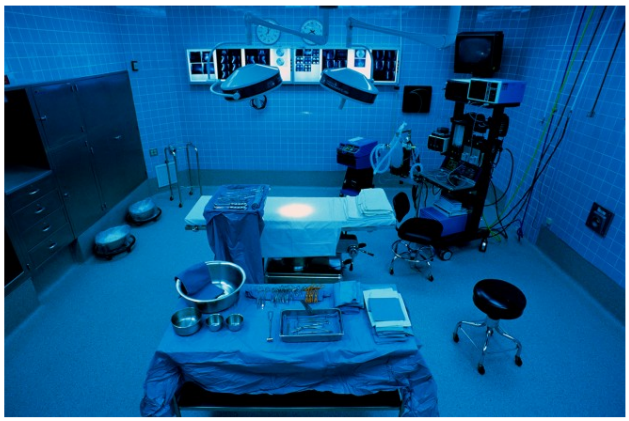


Photo: Charles Thatcher/Getty Images

" … drug infusion pumps ... can be remotely manipulated to change the dosage doled out to patients; Bluetooth-enabled defibrillators … can be manipulated to deliver random shocks to a patient's heart or prevent a medically needed shock from occurring; X-rays … can be accessed by outsiders lurking on a hospital's network; temperature settings on refrigerators storing blood and drugs … can be reset . . . ; and digital medical records … can be altered to cause physicians to misdiagnose, prescribe the wrong drugs or administer unwarranted care. . . ."

From the Investigator Profiled in "It's Insanely Easy to Hack Hospital Systems"

DuaneMorris

So Did We Only Find One?

- Of Course Not. We Found Hundreds!!

Generic Search Examples:

shodan port:445 org:health*/clinic/hospital

health* - http://www.shodanhq.com/search?q=por .health 148 hits

clinic - http://www.shodanhq.com/search?q=port clinic 18 hits

hospital: http://www.shodanhq.com/search?q=por. .hospital 119 hits

medical: http://www.shodanhq.com/search?q=port% medical 255 hits

- Change the search term and many more come up. Potentially thousands if you include exposed third-party healthcare systems.

Source: http://www.slideshare.net/fullscreen/Shakacon/just-what-the-doctor-ordered-part-ii-scott-erven/1

Medical Device Hacking Risks

DuaneMorris

InformationWeek CONNECTING THE BUSINESS TECHNOLOGY COMMUNITY

Home News & Commentary Authors Slideshows Video Reports White Papers Events Univer

STRATEGIC CIO | SOFTWARE | SECURITY | CLOUD | MOBILE | BIG DATA | INFRASTRUC

Partner Perspectives Connecting marketers to our tech communities.

COMMENTARY
4/10/2015
09:55 AM

Liviu Arsene
Partner
Perspectives

Connect Directly

1 COMMENT
COMMENT NOW

Bitdefender
Bitdefender *Perspectives* What's This?

Hacking Vulnerable Medical Equipment Puts Millions at Risk

Hospitals and medical device manufacturers need to start doing more to detect and thwart incoming attacks on networks and devices.

Implantable medical devices are forecast to grow about 7.7% through 2015, and more than 2.5 million people already rely on them to keep various illnesses at bay, according to a study by Freedonia Group.

Medical equipment used to regulate medical conditions has already been deemed vulnerable in various proof-of-concepts, significantly increasing the risk of losing human lives to cyberattacks.

Medical Device Hacking Risks (cont'd)

DuaneMorris

Lack of Basic Security

Today's medical equipment supports everything from Wi-Fi to Bluetooth communication in the hopes of increasing the efficiency of the flow of patient information to medical staff. However, these devices are not properly secured, and most are shipped preconfigured with default passwords such as "password" or "admin," making them worryingly easy to attack.

As part of its research, the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) cited 300 medical devices from 40 companies that had unchangeable passwords. If an attacker were to obtain a list of these passwords, he could theoretically log in and change critical settings, with unfortunate consequences.

Manufacturers that ship these devices are also having a hard time issuing security patches to OTS (off-the-shelf) software, as most medical equipment requiring a software upgrade needs to be resubmitted for FDA approval. Of course, a guidance document specifically states under which conditions a security patch can be issued without immediate FDA approval, but that's still a long way from effectively and proactively updating medical devices across multiple hospitals and countries.

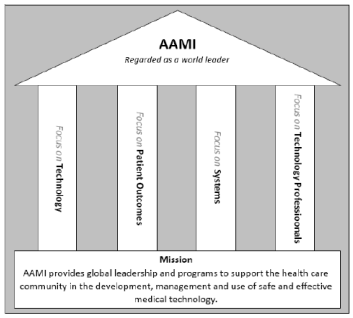
Source: Liviu Arsene, *Hacking Vulnerable Medical Equipment Puts Millions at Risk,* Information Week (April 10, 2015), *available at* http://t.co/94R8Wl9K8o

AAMI
Advancing Safety in Healthcare Technology

Mission: Support health care community in development, management and use of safe and effective medical technology.

AAMI's best role: convening diverse groups to solve problems

Best Known for: **honest broker**



AAMI
Advancing Safety in Healthcare Technology

Challenge: Technology Overload

- No design standardization
- No HDO standardization
- HDOs use old and varied products
- Proprietary features
- Not enough HF
- **Improvements – one hospital at a time**

AAMI
Advancing Safety in Healthcare Technology

Medical Device Risk: Traditional View

- FMEA
- "Normal" use
- Device-by-device
- **Healthcare not viewed as a complex, hazardous sociotechnical system**

AAMI
Advancing Safety in Healthcare Technology

Why We Have to Look at Risk Differently: Integration

- Dispersed regulatory scheme
- Lack of training
- No integrator
- Yet everything is being integrated

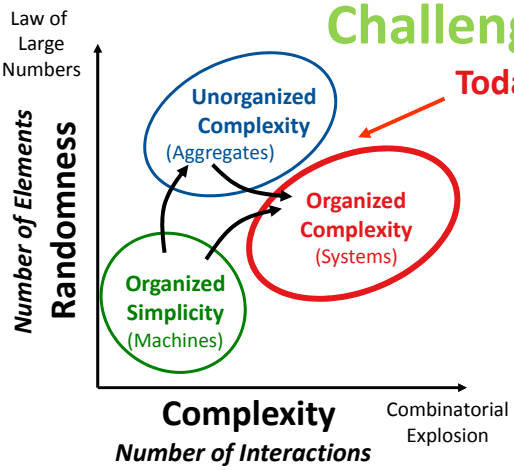
Why We Have to Look at Risk Differently: Culture

- "If you've seen one hospital, you've seen one hospital"
- Rescue model
- Authority
- Many brands, models, eras of devices used in same hospital

Why We Have to Look at Risk Differently: Resiliency

- Resiliency = near misses
- Resiliency = heroes
- Resiliency = can't see inside patient
- Resiliency = workarounds common
- Resiliency = hackers

Organized Complexity: Special Challenges

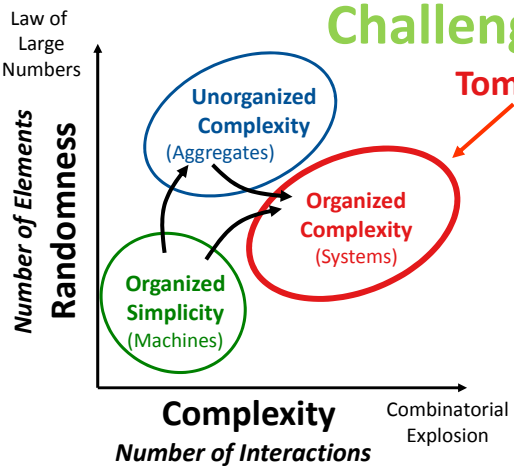


Today we are here

- Losses due to interactions amongst components
- Components work fine
- Unmanaged change evolves to an unsafe state over time

From: G.M. Weinberg, An Introduction to General Systems Thinking, John Wiley & Sons, New York, 1975, p 18. | Many thanks to Lane Desborough, Medtronic, for this slide and the thinking behind it.

Organized Complexity: Special Challenges

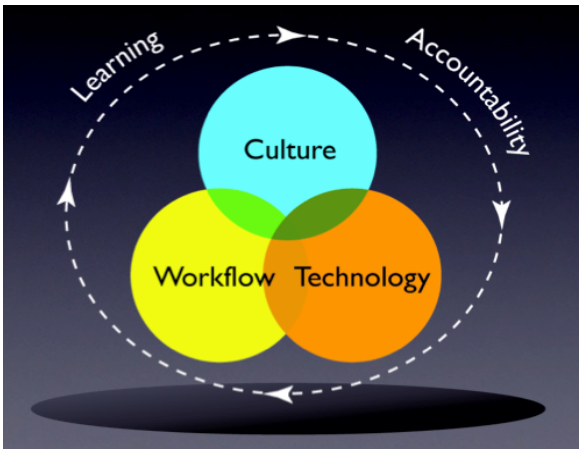


Tomorrow we will be here

From: G.M. Weinberg, An Introduction to General Systems Thinking, John Wiley & Sons, New York, 1975, p 18. | Many thanks to Lane Desborough, Medtronic, for this slide and the thinking behind it.

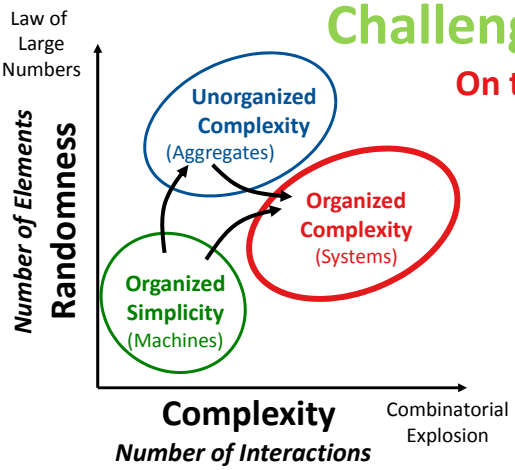
AAMI
Advancing Safety in Healthcare Technology

We Won't Be Cyber Safe Until . . .



AAMI
Advancing Safety in Healthcare Technology

Organized Complexity: Special Challenges



On the horizon …

Horizon

From: G.M. Weinberg, An Introduction to General Systems Thinking, John Wiley & Sons, New York, 1975, p 18.

Many thanks to Lane Desborough, Medtronic, for this slide and the thinking behind it.

"The future is already here, it just hasn't been evenly distributed yet"

– William Gibson

AAMI
Advancing Safety in Healthcare Technology

Working Together to Achieve Cyber Safety

- Think *System* Safety
- Key: stakeholder engagement
- Build Knowledge
- Can't "Fix:" Healthcare is a complex, socio-technical system
- Not one hospital at a time
- Consensus Standards
- Next Generation Products
- It's Not a Project

AAMI
Advancing Safety in Healthcare Technology

Top 10 Ways to Mitigate the Risk and Effects of Cyberattacks on Medical Devices

AAMI's Wireless Strategy Task Force has developed a list of tips for how healthcare organizations can best protect their medical devices and technology. For more resources on wireless technology and cybersecurity, please visit **www.aami.org/hottopics**.

1. Don't leave default passwords in place. Change them!
2. Don't use Wired Equivalent Privacy (WEP), Pre-Shared Key (PSK), or Temporal Key Integrity Protocol (TKIP).
3. Make sure data at rest are encrypted.
4. Have a patch management facility.
5. Employ role-based network access controls.
6. Ensure redundancy.
7. Re-verify system periodically.
8. Perform all of these items on the infrastructure as well.
9. Ask for security test results before purchasing devices.
10. Perform regular audits.

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

VASCULAR SOLUTIONS, INC. & HOWARD C. ROOT,

Defendants.

No. 5:14-CR-00926

MOTION FOR LEAVE TO FILE BRIEF OF CHAMBER OF COMMERCE OF THE UNITED STATES AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE INDICTMENT

The Chamber of Commerce of the United States (the "Chamber") respectfully submits this Motion for Leave to File an *amicus curiae* brief in support of Defendants' Motion to Dismiss the Indictment or, in the Alternative, to Preclude the Government from Using Defendants' Truthful Speech to Prove Misbranding and Adulteration Counts.

1. "No rule or statute defines the trial court's power when determining a motion for leave to file an amicus brief," and thus "'[t]he extent, if any, to which an amicus curiae should be permitted to participate in a pending action is solely within the broad discretion of the district court.'" *Canamar v. McMillin Tex. Mgmt. Servs.*, LLC, No. SA-08-CV-0516-FB, 2009 U.S. Dist. LEXIS 108986, at *2 (W.D. Tex. Nov. 20, 2009) (citation omitted). "[F]actors to consider when determining an amicus request include whether the information offered in the amicus brief is timely or useful, whether the organization submitting the amicus brief is an advocate for one of the parties, and whether the amicus has unique information or perspective beyond what the parties can provide." *Id.* ; *cf.* Fed. R. App. P. 29 (stating that a motion for leave to file an amicus brief should identify "the

movant's interest" and "the reason why an amicus brief is desirable and why the matters asserted are relevant to the disposition of the case").

2. The Chamber has a direct interest in contributing to the sound and principled interpretation of the First Amendment and the Food, Drug, and Cosmetics Act. Specifically, the Chamber's members include pharmaceutical and medical device manufacturers subject to the regulatory regime at issue in this litigation. It thus needs to ensure that its members have the ability to speak truthfully about their products without the threat of criminal prosecution.

3. The Chamber believes that the attached brief will assist the Court in its deliberations. As the world's largest business federation—directly representing over 300,000 members and indirectly representing the interests of more than 3 million companies and professional organizations of every size, in every industry sector, and from every region of the country—the Chamber is able to offer a unique perspective on the First Amendment issues raised by the Government's prosecution.

4. The Chamber is also able to offer the benefit of its experience in litigating commercial speech cases. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. As relevant here, the Chamber has filed amicus briefs in, inter alia, *Sorrell v. IMS Health, Inc.*, 131 S. Ct. 2653 (2011), and *Brown v. Entertainment Merchants Association*, 131 S. Ct. 2729 (2011). Drawing on this experience, the Chamber's brief here both supplements arguments made by the Defendants and provides distinct arguments and authority relevant to those contentions.

5. To avoid any prejudice to the government, the Chamber has timely filed this Motion for Leave to File along with its proposed amicus brief (Exhibit 1) at the same time as Defendants' Motion to Dismiss the Indictment or, in the Alternative, to Preclude the Government from Using Defendants' Truthful Speech to Prove Misbranding and Adulteration Counts.

6. On August 11, 2015, counsel for the Chamber sought the Government's consent to file the attached brief. Counsel for the Government stated that at this time, the Government could not consent to the filing.

7. Counsel for all Defendants consents to the filing of the Chamber's amicus brief.

WHEREFORE, the Chamber respectfully requests that the Court grant this Motion and accept the attached brief.

Dated: August 13, 2015

Basheer Y. Ghorayeb
TX Bar No. 24027392
JONES DAY
2727 North Harwood St.
Dallas, TX 75201
Phone: (214) 969-5069
Fax: (214) 969-5100
bghorayeb@jonesday.com

Counsel for Amicus Curiae Chamber of Commerce of the United States

CERTIFICATE OF SERVICE

I hereby certify that, on August 13, 2015, I caused a true and correct copy of the foregoing document and all attachments to be transmitted via email and UPS Overnight to the Clerk of the United States District Court for the Western District of Texas, San Antonio Division, and a true and correct copy to be sent via U.S. Mail to all counsel of record, including:

Christopher L. Peele
Johnny K. Sutton
THE ASHCROFT LAW FIRM
919 Congress Avenue
Suite 1500
Austin, TX 78701
(512) 370-1800
cpeele@ashcroftlawfirm.com
jsutton@ashcroftlawfirm.com

Jeffrey S. Bucholtz
John C. Richter
KING & SPALDING LLP
1700 Pennsylvania Ave., N.W.
Washington, DC 20006
(202) 626-2907
Fax: (202) 626-3737
jbucholtz@kslaw.com
jrichter@kslaw.com

Michael R. Pauze
KING & SPALDING LLP
1730 Pennsylvania Ave., N.W.
Washington, DC 20006
(202) 626-3732
Fax: (202) 626-3737
mpauze@kslaw.com

Attorneys for Vascular Solutions, Inc.

Dulce J. Foster
John W. Lundquist
Kevin C. Riach
FREDIKSON & BYRON, P.A.
200 South Sixth Street, Suite 4000
Minneapolis, MN 55402
(612) 492-7110
Fax: (612) 492-7077
dfoster@fredlaw.com
jlundquist@fredlaw.com
kriach@fredlaw.com

John E. Murphy
14439 NW Military Hwy., Suite 108-133
San Antonio, TX 78231
(210) 885-2700
johne.murphy@icloud.com

Attorneys for Howard C. Root

Bud Paulissen
Christina Laura Playton
UNITED STATES ATTORNEY'S OFFICE
610 NW Loop 410, Suite 600
San Antonio, TX 78216
(210) 384-7120
Fax: (210) 384-7118
bud.paulissen@usdoj.gov
christina.playton@usdoj.gov

Timothy T. Finley
U.S. DEPARTMENT OF JUSTICE
450 5th Street N.W., 6th Floor, Suite 6400
Liberty Square Building
Washington, DC 20001
(202) 307-0050
timothy.t.finley@usdoj.gov

Attorneys for the United States of America

Basheer Y. Ghorayeb
TX Bar No. 24027392
JONES DAY
2727 North Harwood St.
Dallas, TX 75201
Phone: (214) 969-5069
Fax: (214) 969-5100
bghorayeb@jonesday.com

Counsel for Amicus Curiae Chamber of Commerce of the United States

Exhibit 1

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

VASCULAR SOLUTIONS, INC. & HOWARD C. ROOT,

Defendants.

No. 5:14-CR-00926

MEMORANDUM OF LAW OF CHAMBER OF COMMERCE OF THE UNITED STATES AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE INDICTMENT

Basheer Y. Ghorayeb
TX Bar No. 24027392
JONES DAY
2727 North Harwood St.
Dallas, TX 75201
Phone: (214) 969-5069
Fax: (214) 969-5100
bghorayeb@jonesday.com

Michael A. Carvin
DC Bar No. 366-784
David T. Raimer
DC Bar No. 994558
JONES DAY
51 Louisiana Avenue, N.W.
Washington, DC 20001-2113
Phone: (202) 879-3939
Fax: (202) 626-1700
macarvin@jonesday.com
dtraimer@jonesday.com
**Pro hac vice applications forthcoming*

Counsel for Amicus Curiae Chamber of Commerce of the United States

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

INTEREST OF *AMICUS CURIAE*

The Chamber of Commerce of the United States is the world's largest business federation. It directly represents over 300,000 members and indirectly represents the interests of more than 3 million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. It thus regularly files *amicus curiae* briefs in cases raising issues of concern to the nation's business community.

The Chamber's members include pharmaceutical and medical device manufacturers subject to the regulatory regime at issue here. Consequently, the Chamber has an interest in preserving its members' ability to speak truthfully about their products without the threat of criminal prosecution.[1]

INTRODUCTION AND STATEMENT OF THE CASE

The government has filed criminal charges against Vascular Solutions, Inc. and its CEO, Howard Root, (collectively, "Vascular Solutions") for engaging in truthful, non-misleading speech about so-called "off-label" uses of its Vari-Lase system. Because such an indictment is antithetical to core First Amendment principles, it must be dismissed.

The Food, Drug, and Cosmetics Act (FDCA) regulates the manufacture and distribution of, inter alia, drugs and medical devices. 21 U.S.C. §§ 301-97. Under the FDCA, manufacturers must obtain approval or clearance from the Food and Drug Administration (FDA) before distributing a medical device. *Id.* §§ 360(k), 360c(f), 360e. "As part of the approval [or clearance] process, the FDA . . . reviews the proposed 'labeling' for the drug [or device,] which includes . . . all proposed claims about the [product's] risks and benefits, [its intended use, and] adequate directions for [that] use." *Wash. Legal Found. v. Friedman* ("*WLF*"), 13 F. Supp. 2d 51, 55 (D.D.C. 1998), *appeal dismissed*

[1] No party's counsel authored this brief in whole or in part, and no entity or person, aside from *amicus curiae*, its members, and its counsel, made any monetary contribution intended to fund to the preparation or submission of this brief.

202 F.3d 331 (D.C. Cir. 2000); 21 C.F.R. § 807.87(e). "The FDA will only approve [or clear] the [product] if the labeling conforms with the uses that the FDA has approved." 13 F. Supp. 2d at 55.

Once the FDA approves or clears a device, however, physicians may lawfully use that device for *any* purpose. The FDA does not purport to regulate the practice of medicine (nor is it permitted to do so), 21 U.S.C. § 396, and the agency has long recognized that once a device is approved or cleared "healthcare professionals may lawfully use or prescribe that product for uses or treatment regimens that are not included in the product's approved labeling [or] statement of intended uses." FDA, *Good Reprint Practices for the Distribution of Medical Journal Articles and Medical or Scientific Reference Publications on Unapproved New Uses of Approved Drugs and Approved or Cleared Medical Devices* § III (Jan. 2009), http://www.fda.gov/Regulatory Information/Guidances/ucm125126.htm (hereinafter "*Good Reprint Practices*"). In other words, so-called "off-label" uses are perfectly legal and "generally accepted." *Buckman Co. v. Plaintiffs' Legal Comm.*, 531 U.S. 341, 351 (2001); *WLF*, 13 F. Supp. 2d at 56 (describing this practice as "an established aspect of the modern practice of medicine"). Indeed, the FDA itself has acknowledge[d] that "off-label uses or treatment regimens may be important and may even constitute a medically recognized standard of care." *Good Reprint Practices*, *supra*, § III.

At the same time, the government broadly restricts a manufacturer's ability to make these lawful and beneficial off-label uses known to physicians. In fact, the "FDA has consistently prohibited" manufacturers—and only manufacturers—from "the promotion . . . [of] unapproved uses of approved products." 62 Fed. Reg. 64,074-01, 64,081 (Dec. 3, 1997). The government has created this selective ban on the promotion of off-label uses through an atextual interpretation of the FDCA's prohibition on the "introduction . . . into interstate commerce of any food, drug, [or] device . . . that is adulterated or misbranded." 21 U.S.C. § 331(a). According to the government, if a manufacturer "promote[s a medical device] for a use that has not been approved or cleared by FDA," that medical device is, by definition, "adulterated and misbranded." *Good Reprint Practices*,

supra, § III; *see also United States v. Caronia*, 703 F.3d 149, 154-55 (2d Cir. 2012) (stating that the FDA "has construed the FDCA to prohibit promotional speech as misbranding itself"). The government's theory appears to be that the promotion or marketing of off label-uses creates a new "intended use" for the product, 21 C.F.R. § 801.4, which necessitates supplemental FDA approval or clearance—as well as additional labeling—before the device can be distributed. *See Amarin Pharma, Inc. v. U.S. Food & Drug Admin.*, No. 14-civ-3588, 2015 WL 4720039, at *5 (S.D.N.Y. Aug. 7, 2015).

While manufacturers are thus forbidden from promoting off-label uses, virtually any other speaker may tout the benefits of such uses. The "government's application of the FDCA permits physicians and academics, for example, to speak about off-label uses without consequence, while the same speech is prohibited when delivered by pharmaceutical [or device] manufacturers." *Caronia*, 703 F.3d at 165. In short, the government's regulatory scheme "'has the effect of preventing [manufacturers]—and only [manufacturers]—from communicating with physicians in an effective and informative manner'" regarding the off-label uses of drugs and devices. *Id.* (quoting *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2663 (2011)). Manufacturers who violate this speech ban have been subjected to aggressive prosecutions. *Id.* at 154 (citing examples); *Amarin*, 2015 WL 4720039, at *6-8.

This case is typical of the government's enforcement efforts. Vascular Solutions manufactures and markets the Vari-Lase® Endovenous Laser Procedure Kit, a medical device used to treat varicose veins with laser ablation. Indict. ¶ 11, 12. It is undisputed that the FDA has cleared the use of Vari-Lase devices "for treatment of superficial veins and the Great Saphenous Vein." *Id.* ¶ 12. The FDA, however, maintains that "Vari-Lase devices d[o] not have any form of FDA marketing authorization for treatment of perforator veins"—shorter veins that "connect the superficial and deep vein systems." *Id.* ¶ 13. Despite the fact that it is perfectly legal for doctors to treat perforator veins with the Vari-Lase system, the government has indicted Vascular Solutions for "market[ing]" and "promoting the Vari-Lase system for perforator use." *Id.* ¶¶ 16, 29. Among other

things, the government accuses Vascular Solutions of encouraging its sales employees to provide doctors with "arguments for why lasers were better for treating perforators" than competing products, *id.* ¶ 41, "articles suggesting that lasers were effective at treating perforators," *id.* ¶¶ 41, 54(c), and information regarding "the benefits of [using the Vari-Lase system] for perforator treatment" as well as the "success that other doctors had using the kit for this purpose," *id.* ¶ 53.

In sum, two points are clear. First, the government permits physicians to employ medical devices for any off-label use they find medically appropriate. Second, the government prohibits manufacturers from communicating with doctors regarding such off-label uses. This regime—which allows doctors to treat perforator veins with the Vari-Lase system, but bars Vascular Solutions from giving doctors information on such a use—cannot survive First Amendment scrutiny.

ARGUMENT

The First Amendment precludes the government from prosecuting individuals for engaging in truthful, non-misleading speech, and that ban operates with particular force where the government discriminates on the basis of content or speaker.

As detailed below, the government's ban on off-label promotion is both content and speaker based, and reflects an inherently paternalistic judgment about the information to which trained medical professionals may be exposed. Such regulations cannot be sustained under any form of heightened scrutiny. Where the government has made the decision to allow doctors to use medical devices for off-label purposes and to allow any individual or entity except medical device manufacturers to speak about such uses, it cannot subject manufacturers to a selective criminal ban against conveying truthful and non-misleading information to doctors about the devices they use.

Insofar as the government asserts that it is prosecuting Vascular Solutions for its conduct, rather than its speech, its claims "may be addressed quickly." *WLF*, 13 F. Supp. 2d at 59. As an initial matter, the Supreme Court has squarely held that laws that burden speech, even if ostensibly

regulating conduct, are subject to heightened scrutiny. *Sorrell*, 131 S. Ct. at 2667. In any event, regulation of marketing and promotional activities is regulation of "conduct" only "to the extent that moving one's lips is 'conduct,' or to the extent that affixing a stamp and distributing information through the mails is 'conduct.'" *WLF*, 13 F. Supp. 2d at 59. And even assuming *arguendo* the off-label regime does not facially target speech, the government's past statements, the nature of its prosecutorial activities here and elsewhere, and the essential role a manufacturer's communications play in its theory of liability, eliminate any doubt that the regime is necessarily a speech restriction.

It is thus no surprise that the Second Circuit struck down a similar prosecution on the grounds that the First Amendment prohibits the government from seeking to hold "pharmaceutical manufacturers and their representatives [liable] for speech promoting the lawful, off-label use of an FDA-approved drug." *Caronia*, 703 F.3d at 169. Just last week, the Southern District of New York followed suit, enjoining the government from taking action "against a manufacturer based solely on truthful and non-misleading speech evincing the intent to promote an off-label use." *Amarin*, 2015 WL 4720039, at *23. Here, the government is prosecuting Vascular Solutions for virtually indistinguishable speech—the promotion and marketing of medical devices for off-label uses. This Court should join those courts and hold that prosecution for truthful, non-misleading speech about the off-label uses of medical devices violates the First Amendment. At the least, the canon of constitutional avoidance counsels that the FDCA should not be read to prohibit such speech. *E.g.*, *NLRB v. Catholic Bishop of Chi.*, 440 U. S. 490, 506-07 (1979).

I. CONTENT AND SPEAKER-BASED BURDENS ON TRUTHFUL SPEECH ARE PRESUMPTIVELY UNCONSTITUTIONAL

A. Discrimination on the Basis of the Content of Speech or the Speaker Is Subject to Heightened Scrutiny

Time and again, the Supreme Court has held that restrictions on truthful speech that discriminate based on content and speaker are presumptively invalid, whether those restrictions

burden political speech, commercial speech, or any other speech. *E.g.*, *Reed v. Town of Gilbert*, 135 S. Ct. 2218 (2015); *Sorrell*, 131 S. Ct. at 2671. This result follows from core First Amendment principles. The constitutional protection of speech is premised on the belief "that 'information is not in itself harmful, that people will perceive their own best interests if only they are well enough informed, and that the best means to that end is to open the channels of communication rather than to close them.'" *Sorrell*, 131 S. Ct. at 2671 (quoting *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 770 (1976)). Thus, "above all else, the First Amendment means that government has no power to restrict expression because of its . . . content." *Police Dep't of Chi. v. Mosley*, 408 U.S. 92, 95 (1972). It also means that government may not restrict the expression of certain speakers, because "[s]peech restrictions based on the identity of the speaker are all too often simply a means to control content." *Citizens United v. FEC*, 558 U.S. 310, 340 (2010). Instead, "[t]he First Amendment protects speech and speaker," *id.* at 341, demanding "heightened scrutiny" when the government discriminates against either. *Sorrell*, 131 S. Ct. at 2664.

To avoid heightened scrutiny for a content-based or speaker-based speech restriction, the government must proffer a "neutral justification" for the ban that is unrelated to the message conveyed or to the speaker's identity. *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 429-30 (1993). Several alleged "neutral" justifications are always invalid. For example, the government may not rely on the "justification" that the speaker's expression is "uttered for a profit." *Bd. of Trs. of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 482 (1989). "While the burdened speech results from an economic motive, so too does a great deal of vital expression." *Sorrell*, 131 S. Ct. at 2665. Nor may the government ban a message simply because, in its view, the message would adversely affect its audience. *Linmark Assocs., Inc. v. Twp. of Willingboro*, 431 U.S. 85, 96-97 (1977); *Thompson v. W. States Med. Ctr.*, 535 U.S. 357, 375 (2002). "[T]he fear that people would make bad decisions if given truthful information cannot justify content-based burdens on speech." *Sorrell*, 131 S. Ct. at 2670-71.

For similar reasons, a selective speaker-based restriction cannot be premised on the notion that certain speakers are more influential: here, that manufacturer speech is somehow more likely to lead to off-label uses than speech by other parties. "That the State finds expression too persuasive does not permit it to quiet the speech or to burden its messengers." *Id.* at 2671.

Significantly, the Supreme Court has held that "[c]ommercial speech is no exception" to these anti-discrimination principles because a "consumer's concern for the free flow of commercial speech often may be far keener than his concern for urgent political dialogue." *Sorrell*, 131 S. Ct. at 2664 (internal quotation marks omitted). And "[t]hat reality has great relevance in the fields of medicine and public health, where information can save lives." *Id.* Thus, "strict scrutiny," *id.* (citing *Turner Broad. Sys. v. FCC*, 512 U.S. 622, 658 (1994)), should apply to content and speaker-based burdens on truthful commercial speech just as it does to such restrictions on political speech. *Sorrell*, 131 S. Ct. at 2672.

The Supreme Court's decision in *Sorrell* plainly establishes this rule. There, the Court struck down Vermont's "Prescription Confidentiality Law," which prohibited pharmaceutical companies from using physician prescribing records in their marketing. *Id.* at 2662-63. Critical to the Court's holding was the fact that the Vermont law imposed content and speaker-based burdens on truthful speech promoting prescription drugs. *Id.* at 2663-64. The law disfavored only certain speakers (pharmaceutical manufacturers) and only certain types of speech (pharmaceutical marketing). *Id.* at 2663. Due to this discriminatory treatment, the Court held that it must apply "heightened judicial scrutiny," *id.* at 2664, and that the Vermont law could not survive that scrutiny, *id.* at 2667-72.

Indeed, even before *Sorrell*, the Supreme Court held that "the First Amendment imposes . . . a 'content discrimination' limitation upon a State's prohibition of proscribable speech," like obscenity or defamation. *R.A.V. v. City of St. Paul*, 505 U.S. 377, 387 (1992). Thus, while the government may freely ban all "fighting words," strict scrutiny applies to a content-based ban on

"fighting words" that invoke anger on the basis of "race" or "religion," rather than "political affiliation" or "union membership." *Id.* at 391 ("The First Amendment does not permit [the government] to impose special prohibitions on those speakers who express views on disfavored subjects."). Because strict scrutiny applies to content-based burdens on types of speech (like fighting words or fraudulent speech) that the government may *prohibit entirely*, it *a fortiori* applies to such burdens on constitutionally protected commercial speech.

Here, the ban on off-label promotion is both speaker based and content based, and thus is subject to heightened scrutiny. *See Caronia*, 703 F.3d at 165. The government's prohibition is speaker-based because, as noted above, it allows nearly everyone to discuss the off-label uses of a medical device except for the device's manufacturer. *Supra* p.3. For example, academics may freely discuss those uses in scholarly articles, and many doctors undoubtedly promote those uses in consultations with their patients. Thus, "[t]he explicit structure of the [FDA's regime] allows [off-label promotion] to be . . . [made] by all but a narrow class of disfavored speakers." *Sorrell*, 131 S. Ct. at 2668; *see Caronia*, 703 F.3d at 165. The result is that the government is attempting to subject Vascular Solutions to criminal liability for statements—allegedly encouraging the use of Vari-Lase on perforator veins—that any other speaker could make without fear of prosecution.

The government's ban is content-based because it "applies to particular speech because of the topic discussed or the idea or message expressed." *Reed*, 135 S. Ct. at 2227. In other words, the bar on manufacturer speech pertaining to off-label uses "depend[s] entirely on the communicative content" of the company's marketing. *Id.* Speech discussing *off-label* uses is "disfavor[ed]," while speech on *approved* uses is encouraged. *Sorrell*, 131 S. Ct. at 2663. Worse still, the prohibition is "aimed at a particular viewpoint," *id.* at 2664—namely, the viewpoint that doctors should employ medical devices for an off-label use. The government freely permits speech (by manufacturers or anyone else) to *discourage* off-label uses. *See Caronia*, 703 F.3d at 165.

B. The Prohibition on Off-Label Promotion Cannot Survive Any Form of Heightened Scrutiny

"In the ordinary case it is all but dispositive to conclude that a law is content-based and, in practice, viewpoint-discriminatory." *Sorrell*, 131 S. Ct. at 2667. At that point, strict scrutiny applies, and the government must satisfy the nearly insurmountable burden of "prov[ing] that [its regulations] are narrowly tailored to serve compelling state interests." *Reed*, 135 S. Ct. at 2226. But even if it were to be subjected to the scrutiny typically applied to commercial speech regulations, the government's prosecution of Vascular Solutions cannot pass constitutional muster. Under that test, the government may only proscribe commercial speech if it proves (1) that the speech promotes unlawful activity or inherently misleads its audience, or (2) that the government has a substantial interest; that "the [ban] [on speech] directly advances the governmental interest"; and that it "could [not] achieve its interests in a manner that does not restrict speech, or that restricts less speech." *W. States*, 535 U.S. at 367 (internal quotation marks omitted). This it cannot do.

Indeed, *Western States* essentially controls the analysis on this point. In that case, the Supreme Court applied the commercial speech test to strike down a law that permitted pharmacists to sell "compounded drugs [i.e., drugs modified to meet the needs of a particular patient] without first . . . obtaining FDA approval," so long as they did not advertise those drugs. 535 U.S. at 370. "If they advertise[d] their compounded drugs . . . FDA approval [would be] required" before the drugs could be sold. *Id.* There, as here, a manufacturer's liability turned on his speech. There, as here, the government sought to preclude the public from obtaining information about medical products that were perfectly legal to use. And there, as here, the government's concern was that drug or device manufacturers would circumvent the FDA-approval process. *See id.* at 370-71. Thus, for all the reasons the law at issue in *Western States* could not survive First Amendment scrutiny, the government's prosecution must fail.

1. Speech Promoting Off-Label Uses to Physicians Concerns Lawful Conduct and Is Not Inherently Misleading

The government is free to regulate speech that "concerns unlawful activity," *W. States*, 535 U.S. at 367, or that is "inherently misleading," *In re R. M. J.*, 455 U.S. 191, 203 (1982). Speech about the off-label use of medical devices plainly does not fall into either category. Because the use of a medical device for off-label purposes is entirely *legal*, speech promoting that *legal* conduct does not concern unlawful activity. *See Caronia*, 703 F.3d at 165-66. "[O]nly at such time as off-label [uses] are proscribed by law could the [government] legitimately claim that speech [about those uses] addresses 'illegal activities.'" *WLF*, 13 F. Supp. 2d at 66.

Nor can the government contend that all manufacturer speech about off-label uses is "inherently misleading." *Pearson v. Shalala*, 164 F.3d 650, 655 (D.C. Cir. 1999). If the government were to maintain that "all scientific claims about the safety[and] effectiveness" of off-label uses for medical devices "are presumptively untruthful or misleading until the FDA has had the opportunity to evaluate them," it would "exaggerate [the FDA's] overall place in the universe." *WLF*, 13 F. Supp. 2d at 67. But the government does not so maintain, either in the indictment here or generally. The FDA itself confirms that public health generally benefits from the "dissemination of objective, balanced, and accurate information on important unapproved uses of approved products." 63 Fed. Reg. 64,556, 64,579 (Nov. 20, 1998), and the American Medical Association has indicated that "[i]t is imperative that physicians have access to accurate and unbiased information about unlabeled uses of prescription drugs." 1997 Annual Meeting of the Am. Med. Ass'n, Reports of the Council on Scientific Affairs at 4, https://download.ama-assn.org/resources/doc/csaph/x-pub/csaa-97.pdf.

Indeed, the government cannot rationally maintain that statements about off-label uses are inherently misleading, because the government allows *everyone but the manufacturer* to make those statements. *See Caronia*, 703 F.3d at 165-66. "Were [off-label promotion] either actually or inherently misleading, one would have to conclude that the FDA would be derelict to not proscribe

dissemination under all circumstances." *WLF*, 13 F. Supp. 2d at 68. And, "[u]nder current FDA policy, companies may . . . disseminate information on unapproved uses in response to unsolicited requests for scientific information from health care professionals." 59 Fed. Reg. 59,820, 59,823 (Nov. 18, 1994). If the government thought such communications were always misleading, it could not draw distinctions based on who originated the communication at issue.

Finally, any "inherently misleading" claim is facially implausible because the audience here is not unsophisticated consumers but physicians whom the government itself finds sufficiently knowledgeable to make decisions about unapproved uses. If anything, manufacturer speech should be particularly helpful to physicians given manufacturers' "superior access to information about their [products]." *Wyeth v. Levine*, 555 U.S. 555, 578-79 (2008); 59 Fed. Reg. at 59,823 (manufacturers' "[s]cientific departments . . . generally maintain a large body of information on their products").

2. A Ban on Off-Label Promotion Is Not Necessary to Advance a Substantial Governmental Interest

The government routinely asserts two interests for its ban on off-label promotion—(1) protecting the public health from potentially dangerous uses of drugs or devices; and (2) providing manufacturers with an incentive to get previously unapproved uses on label. Neither suffices to justify the government's broad ban on speech.

Protecting Public Health. If the government has any concerns with the underlying practice of doctors prescribing off-label uses, or with particular types of off-label uses, it is free to regulate those practices. However, having eschewed any direct prohibition on such conduct (because many off-label uses are in fact beneficial rather than harmful), it may not pursue the same purported goal by banning speech. *See W. States*, 535 U.S. at 371. Since the government can claim no valid interest in stamping out the activity promoted by manufacturers' speech, it follows that truthful, non-misleading speech about the activity cannot be harmful in the eyes of the First Amendment. Indeed, by allowing off-label uses while prohibiting speech about those uses, the government has created the

worst of all worlds—doctors are free (and in some cases obligated) to prescribe these uses but are deprived of critical sources of information in their decisionmaking. *Caronia*, 703 F.3d at 167 (noting that the "government's construction of the FDCA essentially legalizes the outcome—off-label use—but prohibits the free flow of information that would inform that outcome").

Indeed, any purported interest in discouraging off-label uses by "keep[ing] people in the dark for what [the government] perceives to be their own good" is automatically invalid. *W. States*, 535 U.S. at 375 (internal quotation marks omitted). "If there is one fixed principle in the commercial speech arena, it is that 'a State's paternalistic assumption that the public will use truthful, non-misleading information unwisely cannot justify a decision to suppress it." *WLF*, 13 F. Supp. 2d at 69-70 (quoting *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 497 (1996) (plurality opinion)). Such paternalism is particularly forbidden because the speech here is directed to sophisticated medical professionals the government entrusts to make informed medical judgments about off-label uses. "[P]rohibiting off-label promotion by a pharmaceutical manufacturer while simultaneously allowing off-label use 'paternalistically' interferes with the ability of physicians and patients to receive potentially relevant treatment information; such barriers to information about off-label use could inhibit, to the public's detriment, informed and intelligent treatment decisions." *Caronia*, 703 F.3d at 166.

In any event, the claim that prohibiting *manufacturer* speech about off-label uses serves a substantial purpose is conclusively undermined by the fact that *everyone else* may engage in precisely the same speech. *Cf. Greater New Orleans Broad. Ass'n v. United States*, 527 U.S. 173, 186-94 (1999) (noting that the government's "unwillingness to adopt a single national policy" on gambling undermined the legitimacy of its interest in "alleviating the societal ills" of gambling and showed that its selective ban on gambling advertisements did not advance that interest).

Incentivizing Manufacturers. Likewise, any interest the government may have in providing manufacturers with an incentive to get off-label uses "on-label" cannot justify the sweeping speech restrictions at issue here. At the threshold, because prior FDA approval of a device's use is concededly not needed to protect the public health (since, as established above, the government *permits* unapproved uses), any interest in having FDA pre-approval of all uses is inherently and concededly not a *public health* interest. That being so, the FDA's desire to pre-approve all uses of approved devices is little more than a self-interested effort to monopolize all decisions about whether a use is safe and effective. The FDCA, however, denies the FDA such monopoly power by recognizing that medical professionals are also capable of making such judgments without the FDA's prior endorsement. *See* 21 U.S.C. § 396. Thus, since the statutory scheme recognizes that the FDA is not the font of all wisdom on unapproved uses, any interest in providing it with this monopoly to the detriment of medical professionals actually undermines the statute's "purpose," and thus cannot be deemed "substantial."

Nevertheless, even assuming that government has a public health interest in establishing an FDA monopoly over doctors' prescribing authority, a ban on providing doctors with truthful, non-misleading information about off-label uses does not directly advance that interest and is not narrowly tailored to achieve it. Even where the government's interests are substantial, "[i]f the First Amendment means anything, it means that regulating speech must be a last—not first—resort." *W. States*, 535 U.S. at 373. Here, because the government targeted speech ostensibly to reduce conduct it has failed to pursue in numerous more direct ways, it cannot show that the speech ban directly advances the government's interest or is narrowly tailored to do so.

First, a speech ban riddled with "exemptions and inconsistencies" concerning the speech and speakers that it covers cannot satisfy the "directly and materially advance" requirement. *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 489 (1995). In *Rubin*, the Court found that a ban on listing alcohol

content in beer labels did not directly advance any government interest because consumers could get that information in other ways. *See id.* Here, as noted, the government's speech ban permits speech encouraging off-label uses from everyone but manufacturers. *See supra* pp. 3, 10-11. Indeed, the government even allows manufacturers to speak about unapproved uses under various exceptions, such as in response to an unsolicited request from a doctor. 59 Fed. Reg. at 59,823. Thus, while a speech ban obviously provides some incentive for manufacturers to proceed through the FDA regulatory process, that incentive is substantially weakened because other entities may fully promote those off-label uses with impunity. If a particular unapproved use has become the standard of care, for example, that information will get to doctors through other channels. As in *Rubin*, therefore, these "exemptions and inconsistencies" call into doubt the government's claim that its speech ban directly advances its interests.

Second, "if the Government could achieve its interests in a manner that does not restrict speech, or that restricts less speech, the Government must do so." *W. States*, 535 U.S. at 371. Here, the government appears to assert that off-label promotion must be banned to avoid the misuse of drugs or devices caused by doctors' lack of accurate information. That assertion is an entirely unsupported and *post hoc* rationalization of the government's enforcement position; however, even accepting it *arguendo*, the government has numerous alternatives at its disposal that restrict less speech. For example, the government could engage in its own speech to "guide physicians . . . in differentiating between misleading and false promotion, exaggerations and embellishments, and truthful or non-misleading information," while reminding them of "the legal liability surrounding off-label . . . treatment decisions."*Caronia*, 703 F.3d at 168. Alternatively, the Supreme Court has "repeatedly point[ed] to disclaimers as constitutionally preferable to outright suppression" of speech. *Pearson*, 164 F.3d at 657. The government could thus require manufacturers, when they speak about unapproved uses, to disclose to physicians that the uses have not been approved by the FDA. Those

disclaimer requirements would provide substantial incentives for manufacturers to obtain FDA approval for those uses, especially if FDA approval is viewed by physicians as important as the government believes it to be. (Conversely, if physicians are indifferent to prior FDA approval, this severely undermines the already weak interest in securing such approval for all uses.) Lastly, the government could "cap[] the amount" of the device that a manufacturer may sell for off-label uses or adopt a "limitation on the percentage of [a device's] total sales that [off-label uses] may represent." *W. States*, 535 U.S. at 372; *Caronia*, 703 F.3d at 167. The First Amendment does not allow the government to impose a flat speech ban without trying obvious alternatives that could directly further its purported interest while restricting less speech.

II. ANY CLAIM THAT THE PROHIBITION ON OFF-LABEL PROMOTION REGULATES CONDUCT RATHER THAN SPEECH IS MERITLESS

Elsewhere, the government has argued that its regulatory scheme does not prohibit speech but only uses it as evidence of "intent" to engage in unlawful conduct. *See Wisconsin v. Mitchell*, 508 U.S. 476, 489 (1993); *Whitaker v. Thompson*, 353 F.3d 947, 953 (D.C. Cir. 2004) (same). This argument has rightly been rejected by every court to consider the question (and by numerous commentators). *E.g.*, *Caronia*, 703 F.3d at 160-62; *WLF*, 13 F. Supp. 2d at 59-60; *Amarin*, 2015 WL 4720039 , at *25; Rodney A. Smolla, *Off-Label Drug Advertising and the First Amendment*, 50 Wake Forest L. Rev. 81, 111-18 (2015); Coleen Klasmeier & Martin H. Redish, *Off- Label Prescription Advertising, the FDA and the First Amendment*, 37 Am. J. of L. & Med. 315, 342-44 (2011).

As an initial matter, even if the government is correct that its regime regulates conduct, not speech, *Sorrell* confirms that it would still be subject to heightened scrutiny. In that case, Vermont made a similar argument—that the "sales, transfer, and use of prescriber-identifying information" at issue in that litigation was "conduct, not speech." 131 S. Ct. at 2666. "[E]ven assuming" that to be true, the Court applied "heightened scrutiny" due to Vermont's content and speaker-based discrimination. *Id.* at 2667. While purporting to regulate conduct, the law imposed "a speaker- and

content-based *burden* on protected expression, and that circumstance [was] sufficient to justify application of heightened scrutiny." *Id.* (emphasis added). Thus, even assuming the regime at issue here does not outlaw speech promoting off-label uses, the government has clearly "impose[d] a speaker- and content-based *burden* on [that] protected expression" by treating such speech as at least partial grounds for criminal prosecution. *Id.* "[T]hat circumstance is sufficient to justify application of heightened scrutiny." *Id.* Indeed, were there any doubt that *Sorrell* subjects the FDA's off-label regime to First Amendment scrutiny, the dissent explicitly acknowledged that the Court's decision would "apply to similar regulatory actions taken . . . by the . . . Food and Drug Administration" and would restrict the government's ability to "control in detail just what a pharmaceutical firm can, and cannot, tell potential purchasers about its products." *Id.* at 2675-76, 78 (Breyer, J., dissenting).

In any event, the "off-label" regime clearly does not use speech to prove impermissible "intent" about proscribed "conduct," because the underlying statutory offense to be "proved"—*misbranding*—is itself a *speech* restriction, and "intent" is not an "element" of the offense under either the FDCA or the FDA's regulations.

Far from being a restriction on "conduct," the "misbranding" prohibition is a government-*compelled speech* requirement, mandating that a product be accompanied by certain government-approved speech on its label. 21 U.S.C. § 352(f)(1); 21 C.F.R. § 801.5 (requiring labeling to include "[s]tatements of all conditions, purposes, or uses for which such device is intended").[2] Moreover, the FDA's (erroneous) interpretation has expanded this speech *compulsion* into a speech *restriction*, effectively forbidding manufacturers from making any statements to doctors that depart from the

[2] On its face, the adulteration provision only prohibits distribution of unapproved devices, 21 U.S.C. § 351(f)(1)(B), which cannot reach Defendants because it is conceded that the FDA has cleared the Vari-Lase system. If the Court accepts the Government's atextual interpretation of that provision to proscribe promotion of approved devices for unapproved uses, it suffers from the same First Amendment flaws as the Government's misinterpretation of the misbranding provision.

government-compelled message on the product's label. Stated differently, the FDCA does not prohibit manufacturers from selling a drug or device with the intent that it be used in a manner not approved by the FDA; rather, on the FDA's theory, the FDCA prohibits the sale of a drug or device without a label that describes the use and directions for use intended by the manufacturer. The underlying offense, especially under the FDA's interpretation, is thus a regulation of speech, not conduct. Accordingly, *Mitchell*'s exception, which allows speech to be used for the limited purpose of establishing "intent" to engage in proscribed "conduct," is clearly inapplicable here.

Mitchell itself makes this clear. There, the Court recognized that while the government could use speech as "evidence of intent" to commit a non-speech-based crime (i.e., battery), it could not do likewise where the underlying regulation itself involved a restriction on expression. 508 U.S. at 487. It thus distinguished *R.A.V.*, where the Court had struck down an ordinance that "only proscribed a class of 'fighting words' deemed particularly offensive by the city—i.e., those 'that contain messages of 'bias-motivated' hatred." *Id.* (quoting *R.A.V.*, 505 U.S. at 392).

In other words, while the Court has narrowly allowed speech to prove the prohibited scienter for non-expressive conduct, it has never endorsed the bizarre principle that speech can be used to "prove" an underlying *speech restriction* without implicating the First Amendment. The underlying speech restriction is *exacerbated* by the *additional* use of the speaker's words to condemn the speaker; it cannot be used to *justify* such hostile use of speech. Smolla, *supra*, at 114 ("[The] evidentiary-use principle is valid *only* when the elements of the underlying crime or tort do not *themselves* require expressive activity. [Then,] it is possible to coherently separate the use of speech as evidence of a nonspeech element from the imposition of liability for the speech itself. When expressive activity is a necessary element of the crime or tort, no such separation is possible."). The government could not, for example, avoid First Amendment scrutiny in a defamation prosecution by claiming to use the defendant's defamatory speech as mere "evidence of defamatory intent,"

because the offense at issue is a speech restriction. Thus, *Amarin* expressly rejected the government's argument that *Mitchell* applies where the underlying offense is based on speech, i.e., "jury tampering, insider trading, [or] blackmail." *Amarin*, 2015 WL 4720039, at *23.

In any event, the "intent" requirement allegedly being "proved" can be found nowhere in the statute—it is solely a *post hoc* interpretation that the FDA devised in order to justify its naked speech restrictions. The government pretends that the FDCA proscribes selling products if the manufacturer has a certain "intent." But that word is not in the misbranding provision. Rather, it prohibits sale of the product unless accompanied by certain *speech*; *i.e.*, a *label* reciting the government-approved uses. *E.g.*, 21 U.S.C. § 352(f)(1). And the FDA's expansion of the misbranding provision is even more obviously a speech restriction; indeed, a content-based one. It effectively forbids manufacturers from saying anything other than what appears on the label. If they echo the label's direction for approved uses, that is permissible. But they can say nothing about an *unapproved use*, even if they echo the label's directions for an approved use. The government obviously cannot justify this pure speech restriction by rewriting the statute to have an "intent to sell" requirement, and then pretending the banned speech is evidence of this invented, proscribed "conduct." This is particularly true since even the FDA's regulations only outlaw a proscribed "objective" intent. 21 C.F.R. § 801.4. Thus, under both the statute and the regulations, the speaker's *subjective* intent—that the "off-label" speech purportedly "proves"—is *irrelevant.*

Western States is again instructive. *Supra* p.9. In striking down a law that made the legality of the sale of compounded drugs turn on whether they had been "advertised," 535 U.S. at 370, the Supreme Court made clear that the government could not transform a speech restriction into a "conduct" prohibition "proved" by speech. Even though—unlike here—the law in *Western States* could have reached the same result if it had been recast as a ban on modifying drugs with the "intent"

to provide them to the general public (with advertising used as "evidence" of this intent), the Court subjected the statute to First Amendment scrutiny and invalidated it. This Court should do likewise.

In reality, the government's intent/conduct argument is nothing more than a sham to justify its regulation of protected expression. For years, the government made no effort to hide that its regulations amounted to a naked restriction on manufacturers' speech. *E.g.*, 74 Fed. Reg. 48,083, 48,087 (Sept. 21, 2009) ("Under the act, companies are prohibited from promoting approved . . . drugs . . . for unapproved uses."); 62 Fed. Reg. at 64,081 (stating that the FDA "has consistently prohibited the promotion of . . . unapproved uses of approved products"); 37 Fed. Reg. 16,503, 16,504 (Aug. 15, 1972) (forbidding "a manufacturer or his representative" from doing "anything that directly or indirectly suggests to the physician . . . that an approved drug may properly be used for unapproved uses"). Likewise, in *Caronia*, the Second Circuit explained that "the government's theory of prosecution *identified* . . . *speech alone* [i.e., marketing and promotion] as the proscribed conduct." 703 F.3d at 159; *see also id.* at 158 & n.6, 160-61 (citing numerous examples). Indeed, the government obtained a jury instruction stating that the "'promotion of [a] drug by a distributor for an intended use different from the use for which the drug was approved by the FDA'" was a criminal offense. *Id.* at 159. Only after courts began to strike down its patently unconstitutional regime did the government's tune begin to change: the language of "promotion" and "marketing" was replaced with the language of "intent." *Compare Good Reprint Practices*, *supra*, § III ("Similarly, a medical device *that is promoted* for a use that has not been approved or cleared by FDA is adulterated and misbranded." (emphasis added)), *with* FDA, *Distributing Scientific and Medical Publications on Unapproved New Uses* § III (Revised Feb. 2014) ("Similarly, a medical device *that is intended* for an unapproved use is considered adulterated and misbranded." (emphasis added)), www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm387652.pdf. This sleight of hand cannot obscure the fact that the government is, and always has been, regulating speech.

The government's claim to be regulating conduct, not speech, is particularly brazen when its only evidence of "adulteration" or "misbranding" is the *speech* of the manufacturer. *E.g.*, Indict. ¶¶ 41, 53, 44 (accusing Vascular Solutions of encouraging its sales employees to provide doctors with "arguments for why lasers were better for treating perforators than . . . competing" products, "articles suggesting that lasers were effective at treating perforators," and information regarding "the benefits of [using the Vari-Lase system] for perforator treatment" as well as the "success that other doctors had using the kit for this purpose"). "[I]f the FDA were truly concerned with the manufacturer's non-expressive act of sale with intent that the product be used off-label, it would logically prohibit *all* sales of a drug [or device] widely used off-label, because *any* time the manufacturer sells its drug [or device], it would do so with knowledge that it will be used for off-label purposes." Klasmeier & Redish, *supra*, at 343. But "there is no indication that the FDA has *ever* pursued a manufacturer for selling its drug [or device] with knowledge that it will be used for off-label purposes, absent off-label promotion." *Id.*; Smolla, *supra*, at 114. "Off-label promotion, then, constitutes both a necessary and sufficient condition for FDA action against a manufacturer." Klasmeier & Redish, *supra*, at 343. Contrary to its claims, therefore, the government "is not seeking to regulate the *act* of sale for the purpose of off-label use; it is, rather, seeking to regulate solely the expression itself—nothing more, nothing less." *Id.*

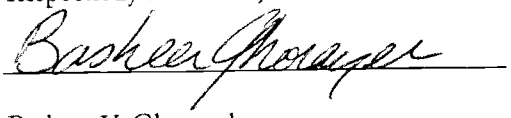
In short, if the government cannot obtain a conviction without establishing that Vascular Solutions promoted Vari-Lase for off-label use, it cannot claim to be regulating anything other than speech. Using the content of a defendant's speech as the *sine qua non* of whether he has engaged in lawful or unlawful conduct is constitutionally indistinguishable from directly outlawing that speech.

CONCLUSION

For these reasons, because the indictment seeks to hold Vascular Solutions liable for truthful, non-misleading speech about off-label uses of the Vari-Lase system, it must be dismissed.

Dated: August 13, 2015

Respectfully submitted,



Basheer Y. Ghorayeb
TX Bar No. 24027392
JONES DAY
2727 North Harwood St.
Dallas, TX 75201
Phone: (214) 969-5069
Fax: (214) 969-5100
bghorayeb@jonesday.com

Michael A. Carvin
DC Bar No. 366-784
David T. Raimer
DC Bar No. 994558
JONES DAY
51 Louisiana Avenue, N.W.
Washington, DC 20001-2113
Phone: (202) 879-3939
Fax: (202) 626-1700
macarvin@jonesday.com
dtraimer@jonesday.com

Counsel for Amicus Curiae Chamber of Commerce of the United States

CERTIFICATE OF SERVICE

I hereby certify that, on August 13, 2015, I caused a true and correct copy of the foregoing document to be transmitted via email and UPS Overnight to the Clerk of the United States District Court for the Western District of Texas, San Antonio Division, and a true and correct copy to be sent via U.S. Mail to all counsel of record, including:

Christopher L. Peele
Johnny K. Sutton
THE ASHCROFT LAW FIRM
919 Congress Avenue
Suite 1500
Austin, TX 78701
(512) 370-1800
cpeele@ashcroftlawfirm.com
jsutton@ashcroftlawfirm.com

Jeffrey S. Bucholtz
John C. Richter
KING & SPALDING LLP
1700 Pennsylvania Ave., N.W.
Washington, DC 20006
(202) 626-2907
Fax: (202) 626-3737
jbucholtz@kslaw.com
jrichter@kslaw.com

Michael R. Pauze
KING & SPALDING LLP
1730 Pennsylvania Ave., N.W.
Washington, DC 20006
(202) 626-3732
Fax: (202) 626-3737
mpauze@kslaw.com

Attorneys for Vascular Solutions, Inc.

Dulce J. Foster
John W. Lundquist
Kevin C. Riach
FREDIKSON & BYRON, P.A.
200 South Sixth Street, Suite 4000
Minneapolis, MN 55402
(612) 492-7110
Fax: (612) 492-7077
dfoster@fredlaw.com
jlundquist@fredlaw.com
kriach@fredlaw.com

John E. Murphy
14439 NW Military Hwy., Suite 108-133
San Antonio, TX 78231
(210) 885-2700
johne.murphy@icloud.com

Attorneys for Howard C. Root

Bud Paulissen
Christina Laura Playton
UNITED STATES ATTORNEY'S OFFICE
610 NW Loop 410, Suite 600
San Antonio, TX 78216
(210) 384-7120
Fax: (210) 384-7118
bud.paulissen@usdoj.gov
christina.playton@usdoj.gov

Timothy T. Finley
U.S. DEPARTMENT OF JUSTICE
450 5th Street N.W., 6th Floor, Suite 6400
Liberty Square Building
Washington, DC 20001
(202) 307-0050
timothy.t.finley@usdoj.gov

Attorneys for the United States of America

Basheer Ghorayeb

Basheer Y. Ghorayeb
TX Bar No. 24027392
JONES DAY
2727 North Harwood St.
Dallas, TX 75201
Phone: (214) 969-5069
Fax: (214) 969-5100
bghorayeb@jonesday.com

Counsel for Amicus Curiae Chamber of Commerce of the United States

Exhibit 2

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. VASCULAR SOLUTIONS, INC. & HOWARD C. ROOT, Defendants.	No. 5:14-CR-00926

[PROPOSED] ORDER

The Court, having considered the Motion for Leave to File Brief of Chamber of Commerce of the United States as *Amicus Curiae* in Support of Defendants' Motion to Dismiss the Indictment, hereby orders that the motion is GRANTED.

The Court hereby directs the Clerk to file the proposed brief forthwith.

_____
U.S. District Court Judge

SECTION H

REGULATORY RISK MANAGEMENT AND MITIGATION (ETHICS CLE)

SheppardMullin

Mitigating Sales and Marketing Compliance Risks: An Enforcement Risk Management Approach

David L. Douglass
Sheppard Mullin Richter & Hampton LLC
2099 Pennsylvania Avenue, NW—Suite 100
Washington, D.C. 20006
ddouglass@sheppardmullin.com
(202) 747-1904

The Compliance Conundrum

- Companies spend more for compliance but no empiric evidence suggests that compliance programs reduce violations
  - More $ recovered by government year after year
- The Question I am most asked by clients
  - How do I know what I don't know?
  - And, how do I prepare for it?
- Compliance Programs manage known risks
- What about unknown risks?
- How do you establish, maintain and adjust compliance policies when the rules have not been set, requirements are uncertain, and standards change?
- How do you manage Enforcement Risk?

SheppardMullin

The Compliance Model

- United States Organizational Sentencing Guidelines
  - Seven Elements of an effective compliance program (see appendix)
- *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959, 970 (1996)
  - Corporations must establish information and reporting systems that are reasonably designed to provide senior management and the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning the corporation's compliance with law and its business performance.
  - On the other hand…

SheppardMullin

The Compliance Model

Obviously the level of detail that is appropriate for such an information system is a question of business judgment. And obviously too, no rationally designed information and reporting system will remove the possibility that the corporation will violate laws or regulations, or that senior officers or directors may nevertheless sometimes be misled or otherwise fail reasonably to detect acts material to the corporation's compliance with the law. But it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility.

In re Caremark International Inc. Derivative Litigation, 698 A.2d at ___ (1996)

SheppardMullin

The Compliance Model

U.S. v. Scientific Application Int'l Corp., 626 F.3d 1257, __ (D.C. Cir. 2010) ("SAIC"), rejecting the "collective knowledge" doctrine

> "the collective knowledge theory allows a plaintiff to prove scienter by piecing together scraps of innocent knowledge held by various corporate officials, even if those officials never had contact with each other or knew what others were doing in connection with a claim seeking government funds."

SheppardMullin

Compliance Model Assumptions

- Rules are known
- Conduct can be controlled
  - Corporate Vicarious Liability Doctrine
- Violations can be eliminated or greatly reduced
- Violations can be detected and remedied before public harm is inflicted
- Legal violations will be rare; sentences will be mitigated

SheppardMullin

The Compliance Challenge

- Compliance tools
  - Policies
  - Education
  - Audits
  - Investigations
  - Corrective Action
- What about unknowns?
  - Known and unknown

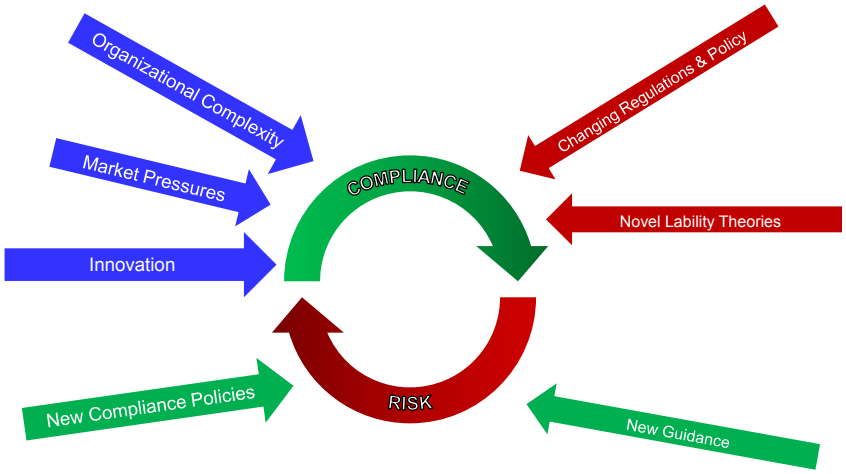
SheppardMullin

Compliance Uncertainty

- Sources
  - Market Dynamics and Innovation
    - Mobile Medical Devices
  - Changing Government Policy
    - Affordable Care Act
    - Sunshine Act
    - Accountable Care Organizations
      - Pay for performance
  - Dynamic Legal and Regulatory Environment
  - Organizational Complexity and Human Imperfection
  - Whistleblowers!!!

SheppardMullin

Compliance/Risk Cycle



SheppardMullin

Compliance vs. Risk Management

Compliance

- Requires certainty
- Yet rejects bright lines
- Binary
- Recognizes imperfection but does not account for it
- Vicarious liability

Risk Management

- Assumes Uncertainty
- Permits a range of conditions
- Accounts for imperfection
- Anticipates and prepares for violations, actual or alleged
- Strives for Balance

SheppardMullin

Enforcement Risk Management

- Risk Management Characteristics
  - Recognizes inevitably of failures
    - Financial
    - Manufacturing
  - Intended to Balance Risk and Reward
- Enforcement Risk Management
  - Recognizes imperfection and the inevitability of uncertainty
  - Anticipates violations, actual or alleged

SheppardMullin

Enforcement Risk Management

- Identify the Knowns
- Recognize the Myth of Certainty
- Identify Sources of Uncertainty
  - Market
  - Organizational
  - Legal and Policy
- Frame and Narrow Uncertainties
- Develop a Regulatory Compliance Risk Management Plan

SheppardMullin

The Enforcement Risk Management Approach

- Understand cornerstones of legal liability
  - *Knowing violation* of an *established, objective standard* that *caused harm*
- Analyze Known Facts According to Established law
- Identify Unknowns
- Understand the Regulatory Environment
- Analyze Enforcement Risks
  - Likelihood
  - Cost
  - Timeline

SheppardMullin

The Enforcement Compliance Risk Management Approach

- Develop Risk Management Plan
  - Identify and Mitigate Risks
  - Engage Stakeholders
    - Business
    - Compliance
    - Legal
- Document the Analysis and Plan
- Monitor Execution
- Objective: Incorporate responding to an enforcement action into your risk management plan

SheppardMullin

The Enforcement Risk Management Approach

- Why is it different?
  - By recognizing the inherent uncertainty in forecasting compliance risks, a risk management model allows companies to better evaluate compliance risk and manage the risk if it materializes.
  - Presumes Compliance Risks can be Reasonably Identified and Managed
  - Continuous vs. Static
  - Sets Compliance Obligations Prospectively Rather Than Retrospectively
    - Shifts Power from Government to Company
  - Higher up-front costs but reduces back-end costs (cost of responding to enforcement action
    - Costs can be internalized
- Enables Company to Factor Compliance Risk into its Business Decisions

SheppardMullin

Appendix

- Elements of an Effective Compliance Program, United States Organizational Sentencing Guidelines, *available at* http://www.ussc.gov/guidelines-manual/2011/2011-8b21

SheppardMullin

7 Elements of An Effective Compliance Program

(a) To have an effective compliance and ethics program …an organization shall--

(1) exercise due diligence to prevent and detect criminal conduct; and

(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

SheppardMullin

7 Elements of An Effective Compliance Program

(b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:

(1) The organization shall establish standards and procedures to prevent and detect criminal conduct.

(2) (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.

(B) High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.

(C) Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.

SheppardMullin

7 Elements of An Effective Compliance Program

(3) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.

(4) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subparagraph (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

(B) The individuals referred to in subparagraph (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.

SheppardMullin

7 Elements of An Effective Compliance Program

(5) The organization shall take reasonable steps—

(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and

(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

SheppardMullin

7 Elements of An Effective Compliance Program

(6) The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

(7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

SheppardMullin

ETHICAL ISSUES ARISING IN HEALTHCARE FRAUD INVESTIGATIONS AND FALSE CLAIMS ACT *QUI TAM* CASES

Robert T. Rhoad, Esq.
Crowell & Moring LLP
Washington, DC

Introduction[1]

The U.S. Department of Justice ("DOJ") announced for fiscal year ("FY") 2013 the second largest recovery in history under the federal False Claims Act ("FCA").[2] The Assistant Attorney General for the Civil Division trumpeted that the DOJ secured $3.8 billion from settlements and judgments in civil cases involving fraud against the government in the FY ending September 30, 2013.[3] This dollar amount brings total recoveries under the FCA since January 2009 to $17 billion, nearly half the total recoveries since the FCA was first significantly amended almost 28 years ago in 1986.[4] As in previous years, the largest recoveries related to healthcare fraud, which reached $2.6 billion.

Pharmaceutical companies and medical device manufactures in particular have been among the healthcare industry participants hardest hit. Of the $2.6 billion in federal healthcare fraud recoveries for FY 2013, $1.8 billion were from alleged false claims for drugs and medical devices under federally insured health programs that include Medicare, Medicaid, TRICARE, veterans' healthcare programs, and the Federal Employees Health Benefits Program. The DOJ recovered an additional $443 million for state Medicaid programs. Many of the recoveries related to allegations that pharmaceutical manufacturers improperly promoted their drugs for uses not approved by the U.S. Food and Drug Administration ("FDA"), commonly referred to as "off-label promotion." The DOJ also resolved allegations relating to the alleged manufacture and distribution of adulterated drugs and obtained 16 criminal convictions and more than $1.3 billion in criminal fines, forfeitures, and disgorgement under the Federal Food, Drug and Cosmetic Act ("FDCA").[5]

With the enactments of the Fraud Enforcement and Recovery Act of 2009 ("FERA")[6] and the Patient Protection and Affordable Care Act ("PPACA")[7] – which expanded the FCA[8] – any entity or individual in the healthcare industry that touches government funds is subject to potential exposure and the heavy sanctions that the FCA imposes. This article discusses ethical issues that attorneys face in managing internal investigations related to healthcare fraud allegations and in handling the pre-unsealing stages of FCA *qui tam* matters that often prompt the government's healthcare fraud enforcement actions.

Ethical Issues in Healthcare Fraud Investigations

Internal investigations have become a common tool for healthcare professionals to detect and prevent misconduct and to respond to allegations of fraud. Much attention is being paid to highly publicized investigation reports relating to well-known corporations that have been the targets of federal enforcement probes (whether conducted under the auspices of the board of directors or by a bankruptcy examiner). Consider General Motors Co., for example, which recently released a 275-page report to its Board of Directors chronicling the results of an investigation overseen by a former United States attorney into the company's handling of a defective ignition switch. The New Jersey Governor, Chris Christie, also released an investigation report concerning lane closures on the George Washington Bridge near Fort Lee, New Jersey, nicknamed Bridgegate. As a result, corporations and corporate directors have become accustomed to call for an internal investigation when there is a suggestion of significant corporate wrongdoing. Yet an internal investigation poses a number of potential risks for the organization, and counsel should be prepared to advise management and the board of those risks before a decision as to whether or how to pursue an internal investigation is finalized.

There are several reasons for management or the board of directors to undertake an internal investigation. The motivation for the investigation will dictate its course and may have an effect on how lawyers engaged in the investigation discharge their various duties. For example, a special litigation committee may conduct an investigation to cut off prospective liability from a derivative action by shareholders. Investigation of potential wrongdoing surfaced through a corporate compliance program may be a preemptive effort to correct the conduct and possibly self-disclose it to an agency. An investigation commenced in the wake of governmental action may be motivated by a desire to demonstrate cooperation, with benefits under federal sentencing guidelines. Counsel, whether internal or external, should be conscious of the client's needs and objectives in guiding the investigation process, and likewise should be aware of the rules of professional responsibility that may govern their conduct.

The dynamics of internal investigations implicate several rules governing the relationship among lawyer, client, and non-clients. These include the independence of the investigatory body and conflicts between and among corporate constituents; creating, protecting and, perhaps, ultimately waiving privilege that might attach to communications with the investigatory body; problems

continued on page 30

Ethical Issues Arising in Healthcare Fraud Investigations

continued from page 29

arising from the investigation of key employees; and coordination between internal and external counsel.[9]

Conflicts of Interest Among Corporate Clients and Constituents

It might seem that a lawyer representing a corporate enterprise can treat the corporation as a single, undifferentiated client. But Model Rule of Professional Conduct ("Model Rule") 1.13, which addresses representation of an organization, is not that straightforward. It provides that a "lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents."[10] Those constituents are the officers, directors, employees and shareholders of a corporation or various committees organized by the board of directors.[11] Where the interests of a corporate client diverge from its constituents, a lawyer who is engaged by the corporation owes his or her duties to the client corporation, and generally may not represent a constituent if the constituent's interests are adverse to those of the organization.[12] Even where those interests are not initially adverse, cautious counsel will refrain from joint representation in order to avoid potential future conflicts.

As Model Rule 1.13 reflects, a corporate organization is a legal construct that acts only through its constituents, *e.g.*, officers and employees. Those individuals may have opposing, differing, or mixed interests, some of which are aligned with the organization's interests and some of which are not, or are only partially so. Their motives may also change. Complicating matters, corporate constituents may not perceive either the organization's interests or their own in the same way as the lawyer does. Finally – and particularly in the case of employees facing potential liability – corporate constituents may have separate counsel who are not bound by duties to the corporation, and who may be working at cross purposes with counsel for the organization.

Model Rule 1.13(g) allows a lawyer to undertake a joint representation of both the corporation and its constituents, subject to the conflict provisions of Model Rule 1.7. If the lawyer becomes aware of a conflict between the interests of the corporation and some or all of the jointly represented constituents, the lawyer must advise the potentially adverse constituents that he or she represents the organization and ensure that the affected constituent understands that the lawyer can no longer provide them legal advice.[13] The lawyer should also advise the constituent that he or she may wish to obtain independent counsel. Care must be taken, the comment to the rule explains, to ensure that the individual understands that the lawyer cannot represent him or her.[14]

A lawyer undertaking a joint representation should be aware of Model Rule 1.7(a), which prohibits a lawyer from representing a client if the representation involves a concurrent conflict of interest, absent informed consent by both affected clients under some permitted circumstances. A concurrent conflict of interest exists if:

1. the representation of one client will be directly adverse to another client; or
2. there is a significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to another client, a former client or a third person, or by a personal interest of the lawyer.[15]

As long as the lawyer does not represent one client in asserting a claim against the other client in the same proceeding, joint representation of clients with a concurrent conflict of interest may be allowed.[16] But this can occur only where the lawyer "reasonably believes that the lawyer will be able to provide competent and diligent representation to each affected client" and each client gives informed consent in writing.[17]

Following Rule 1.7, where there is a concurrent conflict of interest, the lawyer must first make an objective determination that the lawyer will be able to provide competent and diligent representation to both clients and to then obtain informed consent from each client, bearing in mind that there may be some situations where the potential for conflict is so great as to be non-consentable.[18] The comments to Rule 1.7 note, for example, that the substantive law of some states prohibits one lawyer from representing more than one criminal defendant in a capital case.[19] Even where joint representation is allowed and is advisable, the Model Rule requires "informed consent." This means that each client must "be aware of the relevant circumstances and of the material and reasonably foreseeable ways that the conflict could have adverse effects on the interests of that client."[20] This includes the possible effects that joint representation may have on the lawyer's loyalty and confidentiality. There may be situations, however, where it is impossible for one client to reach informed consent, for example, where one client refuses to allow the lawyer to disclose all of the facts the other "client [needs] to make an informed decision."[21]

In general, the joint representation of both a corporation and its constituents can be risky. Even if there is not a direct conflict of interest at the start of the representation, one may develop later, in which case the lawyer will be disqualified from representing one client (and perhaps both). Even where disqualification is not a concern, there are practical considerations. First, courts have broad discretion to disqualify an attorney for actual, or even the serious potential for, conflicts of interest.[22] Second, even when a lawyer is

not disqualified, the government or investigating agency may view joint representation as a sign that the corporation is merely circling the wagons, and may even be perpetuating the very wrongdoing that is under investigation.[23] Third, should corporate counsel ultimately decide to waive the attorney-client privilege, it may be hamstrung in its ability to disclose certain facts to the government if the lawyer's constituent clients refuse to waive the privilege, limiting what the lawyer may disclose.[24]

In FCA investigations and cases, if the constituent has no personal exposure – something the circumstances of the case or government attorneys or agent may be able to make clear – a lawyer may consider "assist[ing] an employee as company counsel while making it clear that there is no joint representation of the company and the employee."[25] But such arrangements are "fraught with risk," especially if the relationship among corporate client, lawyer and constituent are not clearly explained and limited at the outset.[26] The lawyer risks having the constituent claim that a putative attorney-client relationship was formed with the lawyer, even if none was intended or specified. That is one reason, but not the only one, corporate clients may decide to provide separate counsel for their constituents. Sometimes corporate bylaws or state laws require it.

When a lawyer represents solely the corporate entity, and not its constituents, a commonly accepted practice when dealing with constituents during an investigation is for the lawyer to explain the nature of the lawyer's engagement, identify the client, and explain the purpose for the lawyer's inquiries and the manner in which information developed in the investigation will be used and shared. Derivative of the lawyer's obligation under Model Rule 1.13(g), this often involves giving what is referred to colloquially as a Corporate *Miranda* warning – also coined an "Adnarim" warning,[27] *Miranda* spelled backwards – or an "*Upjohn*"[28] warning. Law enforcement officials long ago standardized the form of warnings for arrestees mandated by the *Miranda* decision[29] in the form of a simple printed card. For lawyers, a typical *Upjohn* warning, which can be given verbally to an interviewee and in writing, will likely explain that:

1. The lawyer represents the corporation, not the individual;
2. The lawyer's obligations are to the corporation, not the individual;
3. The communications between the lawyer and individual may be privileged on behalf of the corporation, and only the corporation, not the individual, may waive that privilege; and
4. The corporation may waive its privilege and disclose what the individual tells the lawyer to anyone it chooses.[30]

Afterwards, it is prudent to memorialize that an *Upjohn* warning was given to and understood by the constituent. The mere fact of the warning itself may have the effect of discouraging the very cooperation the lawyer requires to conduct an appropriate investigation. But many currently-employed constituents will want to assist their company in the investigation and nonetheless cooperate.[31] Better to ensure that the constituent understands the lawyer's role, than risk creating confusion – and conflict – later on.

Privilege Considerations with Corporate Constituents

Many of the most challenging issues surrounding internal investigations center on the applicability of the attorney-client privilege to the internal investigation process and, concomitantly, the preservation of that privilege unless and until the time comes to waive it.[32] Even though the end result of many internal investigations is the disclosure of the investigation's results to the government, a corporate client would typically prefer to have some control over the timing and manner of any such disclosure. However, even though the rule "the privilege belongs to the corporation" seems straightforward, the privilege may be inadvertently lost in surprising ways.

The concept of the corporate attorney-client privilege has always been difficult in application. Before the Supreme Court's *Upjohn* decision, a number of courts followed the "control group" test, and some state courts still do, which essentially limited the privilege to communications between the corporation's attorneys and the limited group of corporate officers who were in a position to determine and direct the corporation's response to legal advice rendered.[33] In this formulation, even communications with senior corporate officials might be outside the protection of the privilege if those officials were outside the chain of command with respect to the matter at issue. *Upjohn* abandoned the control group test in federal courts in favor of a facts-and-circumstances analysis. While the Supreme Court declined to adopt a bright line rule of privilege, its decision in *Upjohn* focused on several factors, such as whether (i) the allegedly privileged communication was made to counsel, acting as such, (ii) the allegedly privileged communication was made at the direction of corporate superiors to secure legal advice, (iii) the information sought or communicated concerned matters within the scope of the employees' corporate duties, and (iv) the employees were aware that they were being questioned so that the corporation could obtain legal advice.[34] These factors guide courts in determining privilege claims.

The absence of a bright-line test after *Upjohn* means there can be no assurance that a tribunal will agree that a particular communication with a particular person within the corporation is privileged. This uncertainty was recently highlighted when a large government contractor, Kellogg Brown & Root, Inc. ("KBR"), was ordered to produce internal investigation reports that

continued on page 32

continued from page 31

had been prepared for in-house counsel in response to employee complaints about possible misconduct in Iraq.[35] Even though the investigative reports were prepared at the direction of counsel and kept under lock and key in the company's legal department, the district court concluded that KBR's reports were not privileged and had to be produced to the relator in a *qui tam* FCA case.[36]

KBR filed a petition for a writ of mandamus shortly afterwards, which the D.C. Circuit granted, vacating the district court's discovery order.[37] In its opinion, the D.C. Circuit rejected the district court's application of a but-for test for determining privilege – which meant, according to the district court, that investigation reports were privileged only where legal advice was the but-for cause of the investigation. The D.C. Circuit held that the attorney-client privilege applies so long as "one of the significant purposes of the internal investigation was to obtain or provide legal advice," even if it was not the sole, triggering purpose.[38] The court noted that the privilege applies regardless of whether the investigation was conducted under a "company compliance program required by statute or regulation, or was otherwise conducted pursuant to company policy."[39]

While the D.C. Circuit's decision is a welcome one for organizations operating in regulated industries such as healthcare organizations which may perform investigations for dual purposes, both business and legal, it is not be the final word. It remains to be seen if courts in other jurisdictions will follow the D.C. Circuit. It is therefore prudent for healthcare organizations to implement practical measures to strengthen attorney-client privilege claims, which may help avoid having to litigate these complex issues to begin with.[40] Because there is no bright-line rule after *Upjohn*, questions about the scope of the attorney-client privilege will continue to be answered on a case-by-case basis, making attorney involvement in internal investigations critical if the privilege is to apply.

Special Problems with Employees: The Right to Counsel

Situations involving potential criminal liability for corporate executives require consideration of difficult issues. In these situations the individuals may require separate counsel from the corporate defendant, and in many cases are the beneficiaries of indemnification – required by state law, contract, or corporate bylaws –which entitles them to counsel at the expense of the corporation. For example, "Delaware law requires that its corporations indemnify present or former officers and directors who are 'successful on the merits or otherwise in defense' of any such legal action."[41] The situation becomes cloudier when the conduct of the defendant raises serious questions of whether he/she was acting in the course and scope of his/her employment or may have engaged in criminal behavior. Many indemnification agreements or state laws provide the corporation a basis for denying payments for counsel in circumstances where the executive has breached duties to the corporation (subject to a right of the executive to recover if he or she is exonerated). In Delaware, "a corporation is *prohibited* from indemnifying its officers and directors if they acted in bad faith or in a manner that they did not reasonably believe was in . . . the best interests of the corporation."[42]

The problem of advancing legal fees and the provision of separate counsel to employees has implications under Model Rules 1.7 and 1.13 in that (i) interests of the employees and the corporation may diverge to such a degree that a joint privilege or a common defense strategy cannot be created or preserved, and (ii) the interests of the employee may be injured if the lawyer proceeds in a manner consistent with the interest of his or her corporate client and divulges information to senior corporate officials that implicates the employee. As a practical matter, effective legal representation in a white-collar fraud cases is costly, and paying the cost of counsel can be a substantial financial burden even on highly compensated employees.

It is sometimes suggested that if an employee did nothing wrong, he or she does not need separate (and sometimes expensive) representation and that advancement should not be an issue. But such a position does little to reassure an employee who fears, rightly or wrongly, that he or she may be offered up as a sacrifice to protect the organization or more senior individuals. And it assumes that such a decision can be made upfront, before a thorough investigation has been completed, which is not necessarily true in complicated situations or where the peculiar facts of what happened are unknown. Judging an employee's potential risk without an understanding of what happened may be difficult depending on the person's position and responsibilities. Where multiple employees may need separate counsel, some corporations will suggest that one law firm serve all of them, as pool counsel, which may lessen the total fees incurred and increase information-sharing among the individuals and corporation. While pool counsel may create efficiencies, corporate counsel should vigilantly be on the lookout for conflicts among these employees and recognize that enforcement officials "frown[] upon joint-defense agreements with potentially culpable employees that might result in the sharing of information about the government's investigation."[43]

Coordination Between In-house and Outside Counsel

Beyond the internal and external counsel for the organization itself, a

major investigation is increasingly likely to involve a variety of other lawyers. In addition to lawyers for individual targets and defendants, other constituencies may well bring in separate counsel. After the rash of corporate scandals beginning with the collapse of Enron Corporation, and particularly after the passage of the Sarbanes-Oxley Act,[44] there has been an intense focus on "independent" legal advice for corporate boards and their committees.[45] In a crisis potentially implicating senior management, internal counsel and their regular outside counsel should expect that the board of directors, the outside directors, the audit committee or other subgroups of the board may feel the need to bring in independent counsel in addition to counsel engaged to represent the organization.[46]

Ethical Issues that May Arise in FCA *Qui Tam* Cases

The complicated nature of *qui tam* litigation, which involves multiple parties – the relator, government customer, government enforcement body, and defendant – presents unique ethical and legal challenges at each stage of litigation for the lawyers representing both relators and defendants. This section addresses some of the issues that arise in the early stages of *qui tam* litigation.

Ethical Issues that Arise Before a Qui Tam Complaint is Filed

A *qui tam* action is initiated when a relator serves a copy of the complaint and a written disclosure of substantially all of the material evidence and information the relator possesses to the DOJ.[47] The complaint is first filed *in camera*, not on the public docket, where it remains under seal for at least 60 days, before it is served on the defendant. A lawyer that is approached by a putative relator should be guided by several ethical considerations before deciding to file a *qui tam* complaint.

Duty to Refrain from Filing Frivolous Suits

The overwhelming majority of new FCA cases, referrals, and investigations are initiated by relators – nearly 90 percent in fiscal year 2013 – who approach a lawyer with allegations that their current or former employer engaged in misconduct involving government funds. The risk that such a putative relator may be motivated by animosity, the possibility of receiving a financial windfall, or a desire to seek reprisal against his or her [or 'the'] former employer means that a lawyer must investigate whether there is a sound basis for bringing the suit. A lawyer who fails to heed the multiple ethical obligations involved in avoiding filing a frivolous suit risks professional discipline, personal liability, and court-imposed sanctions.

– *Model Rule of Professional Conduct 3.1*

Rule 3.1 of the Model Rules provides that lawyers should not "bring or defend a proceeding, or assert…an issue…unless there is a basis in law and fact for doing so that is not frivolous…."[48] The fact that a putative relator may harbor motives other than vindicating perceived wrongdoing does not render the allegations or action frivolous, and a lawyer need not actually believe that his client's position will ultimately prevail.[49] The Comments to the Rule make clear that what is required of the lawyer is to "inform themselves about the facts of their clients' cases and the applicable law and determine that they can make good faith arguments in support of their clients' positions."[50] An action is not frivolous merely because the person's allegations "have not been fully substantiated or because the lawyer expects to develop vital evidence only by discovery."[51] But the lawyer should undertake some investigation of the person's allegations to ensure that his or her position can be supported by arguments made in good faith.

– *Model Rule of Professional Conduct 1.1*

A lawyer's success in complying with Rule 3.1 is closely linked to meeting his or her obligation to provide competent representation under Rule 1.1. Competent representation "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[52] As the Rule's comment explains, competence rests in part on the lawyer's thoroughness and preparation: "Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem. . . ."[53] Like Rule 3.1, Rule 1.1 encourages lawyers to examine the facts of their particular case.

– *Federal Rule of Civil Procedure 11(b) and 28 U.S.C. § 1927*

A third rule that addresses a lawyer's duty to avoid filing frivolous claims is found in Rule 11 of the Federal Rule of Civil Procedure ("FRCP"). Under Rule 11(b), a lawyer filing a complaint is certifying that "to the best of the person's knowledge, information, and belief" – based on "an inquiry reasonable under the circumstances" – the factual allegations or claims "have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery." This rule is not intended to be "applied to adventuresome, though responsible, lawyering which advocates creative legal theories."[54] But it does impose on the lawyer a duty to conduct a reasonable and competent inquiry, similar to Model Rule 1.1, before signing a complaint.[55] This is a continuing duty to inquire, one that does not end at the case's filing, and which applies to discrete portions of a pleading, not just to the complaint as a whole.[56]

The procedural and substantive complexity of FCA litigation may, especially for an attorney who lacks *qui tam* litigation experience, make the risk of not recognizing a frivolous

continued on page 34

continued from page 33

claim perilous. A lawyer should be aware of and understand not only the facts of the client's case and the elements of a cause of action under the FCA, but also the procedural requirements. For instance, a lawyer not familiar with the FCA's seal provision might inadvertently violate the statute by filing a *qui tam* case on the public docket or fail to make the required disclosure to the DOJ. The lawyer may risk facing professional discipline for violating the ethics rules, as well as sanctions for violating Rule 11.[57] Moreover, under 28 U.S.C. § 1927, district courts have authority to impose sanctions on attorneys *personally* for costs, expenses and attorneys' fees reasonably incurred because of an attorney who "multiplies the proceedings in any case unreasonably and vexatiously."[58]

– 31 U.S.C. § 3730(d)(4)

In addition to the rules outlined above, the *qui tam* provisions of the FCA contain their own deterrent to the filing of frivolous claims. Section 3730(d)(4) provides that if the government does not intervene and the relator conducts the action on his or her own "[a] court may award to the defendant its reasonable attorneys' fees and expenses if the defendant prevails in the action and the court finds that the claim of the person bringing the action was clearly frivolous, clearly vexatious, or brought primarily for purposes of harassment."[59] While the FCA does not define "clearly frivolous," courts have offered varying definitions that suggest that the standard is whether the FCA claims had any objectively reasonable chance of success.[60] Section 3730(d)(4) does not apply to awards against an attorney,[61] but courts have assessed attorneys' fees against whistleblowers under this provision in a number of cases.[62]

FCA litigation is one of the few commercial litigation areas that departs from the American rule regarding attorneys' fees and costs, under which each party to a proceeding bears its own fees and costs. In FCA cases there is a risk that the non-prevailing party will have to pay the other side's attorneys' fees. A lawyer evaluating a client's FCA claim would therefore be prudent to consider his/her ethical obligations of competence under Model Rule 1.1 in advising the client of the risk that he/she could end up owing thousands of dollars in attorneys' fees and costs to the defendant. Such guidance may be warranted even after the case has been filed, when further investigation or discovery plainly disproves the client's allegations. Even without express statutory authority, federal courts have inherent powers to impose attorneys' fees against the losing party "when the losing party has acted in bad faith, vexatiously, wantonly, or for oppressive reasons."[63]

– First-to-File Rule and Model Rule of Professional Conduct 1.3

One of the challenges facing a lawyer who seeks to ensure that a putative relator's claim is not frivolous is that the lawyer may have limited time to investigate before making the decision to file the *qui tam* complaint. Rule 1.3 of the Model Rules requires that a lawyer act "with reasonable diligence and promptness in representing a client." Compounding this rule is § 3730(b)(5) of the FCA, which is commonly referred to as the "first-to-file" bar. Under this provision, if another relator has previously filed an FCA complaint making related allegations based on the same facts, the district court will dismiss the second action.[64] The Fifth Circuit has explained that "as long as the later-filed complaint alleges the same material or essential elements of fraud described in the pending *qui tam* action," the later-filed action is jurisdictionally barred.[65] An attorney contemplating initiating a *qui tam* action must balance the ethical duties requiring the attorney to avoid filing a frivolous complaint with the risk that waiting too long to file could mean that his/her client's case might be dismissed under the first-to-file bar if another case alleging the same material elements of fraud is filed first.

– Model Rule of Professional Conduct 1.16

Conventional wisdom holds that the best outcome for relator's counsel in any *qui tam* action is to convince the government to intervene, since in that event the action will be litigated by experienced DOJ attorneys, which often leads to quick and larger settlements. While § 3730(b) of the FCA allows private citizens to file *qui tam* actions, if the government elects to intervene during the 60-day period or any extension of that period, from that point forward the "action shall be conducted by the Government."[66] Because of the frequency with which the government does not intervene in *qui tam* actions, however, a lawyer considering whether to take on representation of a relator would be prudent to add Model Rule 1.16 to the list of ethical obligations to consider prior to filing a complaint, particularly if the lawyer lacks experience litigating *qui tam* actions.

Rule 1.16 provides the circumstances in which a lawyer can withdraw from a client's representation.[67] But even if the lawyer can show "good cause" for withdrawal, Rule 1.16(c) provides that the lawyer may be ordered by a court to continue representation "notwithstanding good cause for terminating the representation."[68] Before filing a complaint in a *qui tam* action, a lawyer should be prepared for the possibility that there may be no easy way out of the representation. Lawyers who know that they may not want (or be able) to litigate a case through trial without government intervention may seek to insulate themselves by providing in the retention letter that they can

withdraw if the government declines to intervene.[69]

Ethical Challenges in Investigating Allegations While the Case is Under Seal

The seal provisions of the FCA are set forth in § 3730(b)(2), which provides that "a copy of the complaint and written disclosure of substantially all material evidence and information" the relator has must be served on the Government and that "[t]he complaint shall be filed in camera [and] shall remain under seal for at least 60 days." Once the complaint is filed it remains under seal for at least 60 days while the government investigates to determine whether or not it will intervene. During this seal period, the complaint is not served on the defendant. Relator and his/her counsel are subject to sanctions by the court if they violate the seal, including dismissal. The seal provisions add more complexity to the ethical considerations facing FCA counsel. Like any attorney, relator's counsel must conduct an investigation of the facts thorough enough to meet the ethical standard of competence to his client, as well as his/her duty to avoid filing a frivolous complaint. Relator's counsel, however, must meet all of these duties while staying within the unique statutory restrictions of a pending action that client and counsel cannot reveal to or discuss with others.

Duty to Respect the Rights of Third Parties

In order to gather evidence beyond a relator's word to support allegations that the elements of the FCA violation are met, counsel often seek company documents and contact with a defendant organization's employees. Both involve ethical challenges that place the lawyer's duty to provide competent representation in tension with rights owed to third parties, as well as with his/her obligation to conform to requirements of the statute while the complaint remains under seal. During the seal period, "the normal methods of gathering evidence prior to trial, including the taking of pre-filing depositions and the gathering of…records…are simply not available. [A]bsent smoking gun documents from the relator, the case hinges in large measure on the credibility of the relator and his knowledge of incriminating documents that the United States Attorney might be able to obtain by subpoena."[70]

In healthcare cases, the attorney has an added concern: The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which governs the privacy of protected health information. An attorney should be mindful that his/her client may have taken and still possess confidential and HIPAA-covered documents, some or all of which may be covered by a separate confidentiality agreement with the client's employer. This means that a lawyer representing a relator must be careful to understand what material, if any, his or her client removed from the workplace and whether it contains protected health information that is subject to a confidentiality or nondisclosure agreement. Some relators have faced counterclaims after filing an FCA suit once their employer (or former employer) discovers that the relator disclosed confidential and HIPAA-protected material that was subject to a confidentiality agreement.[71]

– Contacting Witnesses Other Than the Relator – Model Rule of Professional Conduct 4.2

Model Rule 4.2(b) provides that "[i]n representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter [concerning the matter], unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order."[72] The rule requires that the lawyer have knowledge that the person is, in fact, represented in the matter to be discussed.[73] Knowledge, however, may be inferred from the circumstances.[74] In the context of an FCA case, counsel for the company may represent not only the company, but some or all of its employees, or there may be outside counsel specifically retained to represent the employees. As such, under this Rule counsel for the relator may have an ethical duty not to contact employees without consent of the person's counsel.[75] If doing so, however, the relator's counsel should be careful not to inadvertently violate the FCA's seal provisions. Waiting for the case to be unsealed may be a safer alternative.

Model Rule 4.2 is another instance in which a state's rules of ethics may differ from the Model Rules. For example, some commentators argue that the District of Columbia's version of Model Rule 4.2 is more lenient than the Model Rule.[76] Specifically, D.C. Rule 4.2(b) states that:

> During the course of representing a client, a lawyer may communicate about the subject of the representation with a nonparty employee of an organization without obtaining the consent of that organization's lawyer. If the organization is an adverse party, however, prior to communicating with any such nonparty employee, a lawyer must disclose to such employee both the lawyer's identity and the fact that the lawyer represents a party that is adverse to the employee's employer.[77]

Under the D.C. Rule, a "party" is defined in 4.2(c) as "any person or organization, including an employee of an organization, who has the authority to bind an organization as to the representation to which the communication relates."[78] Thus, the D.C. Rule does not bar contact with employees who do not have authority to bind a corporation. Model Rule 4.2, in contrast, concerns "persons" without distinguishing among employees and would allow in-house

continued on page 36

continued from page 35

and defense counsel to argue that contact by opposing counsel is prohibited over a wider group of employees.[79] Thus, counsel should be aware of state rule variations on Model Rule 4.2 and other rules of professional conduct in assessing whether the conduct in question meets their ethical obligations. Counsel must also keep in mind that a lawyer cannot make a communication prohibited by Model Rule 4.2 through the acts of another,[80] and may be subject to discipline for misconduct if he or she knowingly assists or instructs an agent to violate or attempt to violate any of the Model Rules.[81] Finally, even if permission is given or is not required, a lawyer should be careful not to obtain *documents or evidence* in a manner that violates the legal rights of the organization under Model Rule 4.4.[82]

– *Accepting Company Documents Obtained by the Relator – Model Rule of Professional Conduct 4.4*

FCA cases typically rest on documentary evidence to support allegations. Because normal discovery channels are closed while the case is under seal, counsel must be aware of his/her ethical obligations in accepting and using unsolicited, unauthorized confidential or privileged documentary evidence obtained from the alleged wrongdoer.

Model Rule 4.4(a) states that, "[i]n representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person." Although the Rule does not "catalogue all such rights," it does note that such rights "include legal restrictions on methods of obtaining evidence from third persons and unwarranted intrusions into privileged relationships, such as the client-lawyer relationship."[83] There is scarce guidance under the Model Rules and in ethics opinions on this issue, which leaves attorneys guessing as to how to balance their duties of competent representation with the third party rights of the client's employer.

In 1994, the American Bar Association ("ABA") initially rendered an opinion characterizing the unauthorized review of privileged or confidential information as misconduct. Basing its reasoning on an opinion related to inadvertent disclosure under Model Rule 4.4(b),[84] the Formal Opinion advised lawyers who "without solicitation, receive materials which are obviously privileged and/or confidential" that they had a "professional obligation to notify the adverse party's lawyer that [he or] she possesses such materials and either follow the instructions of the adversary's lawyer with respect to the materials, or refrain from using the materials until a definitive resolution of the proper disposition of the materials is obtained from the court."[85] In 2006, the ABA withdrew this Opinion without providing guidance as to what professional obligation is owed by an attorney confronted with this scenario, except to say that "[w]hether a lawyer may be required to take any action in such an event is a matter of law beyond the scope of the Rule 4.4(b)."[86]

More recently, in August 2011, the ABA issued a Formal Opinion on a lawyer's duty under Model Rule 4.4(b) when, during the course of a lawsuit, he/she receives copies of a third party's email communications with counsel that were *not* inadvertently sent, such as in the hypothetical scenario of an employer who receives copies of an employee's private communications with counsel after the employee filed a lawsuit against the company, and the emails were located in the employee's business e-mail file or on the employee's workspace computer or other device. The Opinion concluded that because such privileged communications were not sent "inadvertently," Model Rule 4.4(b) does not apply to this circumstance and therefore does not require notice to opposing counsel other than in the situation that Model Rule 4.4(b) expressly addresses (inadvertent disclosure).

Thus, the ABA guidance on the issue appears to suggest that if a lawyer receives materials which are privileged or confidential (without solicitation), he or she has no ethical obligation under the Rules to notify the adverse party's lawyer or seek an order from the court on the proper disposition of the materials. The ABA has been careful to note that the fact that the Model Rules do not impose an ethical duty to disclose to opposing counsel receipt of private, potentially privileged e-mail communications between an opposing party and his/her counsel does not mean that courts cannot or should not impose a disclosure obligation pursuant to their supervisory or other authority.[87] In addition, lawyers should keep in mind that individual states may have differing interpretations of the rule which dictate different outcomes.

A case from the United States District Court for the District of Arizona, *U.S. ex rel. Frazier v. IASIS Healthcare Corp.*, provides helpful instruction, particularly in the context of an FCA case that is under seal.[88] In *Frazier*, a *qui tam* action was filed by a former Chief Compliance Officer who, prior to leaving employment, copied and removed "1,300 pages of documents, emails and other [company] proprietary materials" without authorization.[89] During the course of reviewing these documents, relator's counsel came across documents which "contained legends such as 'attorney client privilege' or had information on the header indicating that they might contain privileged or attorney work-product information."[90]

Relator's counsel argued that they set the documents aside and later had a paralegal segregate them into a sealed box. In addition, they claimed that they had neither read nor relied on any of the documents in preparing the complaint. A month after the case was unsealed, counsel for the defendants sent a letter stating that certain documents protected from disclosure by the attorney-client and work-product privileges had been misappropriated and demanded that they be returned. Relator's counsel ultimately advised the relator that since the seal was lifted, the documents could be returned. The defendants pointed out, however, that relator's counsel initially responded to the demand letter in a manner that suggested that they were not aware that any potentially privileged or confidential documents were in their possession.[91]

After the case was dismissed, defendants sought sanctions and attorneys' fees against relator's counsel, asserting: "*Qui Tam* Counsel had ethical duties not to review, retain, disclose, or use the privileged material that they received from [relator]" and that they had a duty to notify the defendants of the privileged materials when received and either return them or seek a ruling from the court regarding the materials.[92] The relator's counsel relied on an Arizona State Bar Ethics Opinion that stated that a lawyer who receives from his or her client copies of documents that belong to the adversary and appear, on their face, to be subject to the attorney client privilege or to be otherwise confidential is obligated: "(i) to refrain from further examination of the material or from making use of it, (ii) to notify opposing counsel of its receipt, and (iii) either to abide by that counsel's instruction as to its disposition or to seek a ruling from a court as to whether it may be used."[93] The Opinion went on to state that "[w]hen no litigation has been brought, and presumably cannot be brought, the lawyer should refrain from reviewing or making use of the information in the documents and notify the ex-employer's counsel that they have come into the lawyer's possession."[94] The Opinion also noted that Arizona Ethics Rule 1.6 "requires client consent before the lawyer may notify the ex-employer or its attorney that the lawyer has received privileged or confidential material belonging to the ex-employer" and if the client refuses permission, the "lawyer still should refrain from examining the documents or making use of the information in them."[95]

The court found that the Arizona ethics opinion was not directly on point in the FCA context because 31 U.S.C. § 3730(b)(1)(2) requires that the complaint be filed under seal for at least 60 days and prohibits the relator from serving the defendant with the complaint until the court so orders. Hence, "upon discovering that they had potentially privileged documents from [the defendant], *Qui Tam* Counsel could not reveal the potential lawsuit" prior to unsealing the complaint and could therefore not be sanctioned for failing to inform the defendants that they had potentially privileged documents prior to the complaint being unsealed. The court went on, however, to state that the fact the case was under seal did not relieve relator's counsel from the obligation to seek a ruling from the court as to what to do with the privileged documents. Since the relator's counsel never sought such a ruling on the privileged documents, the court found that "*Qui Tam* Counsel did breach an ethical duty to seek a ruling from the court about the privileged documents and breached their duty to contact [the company] about the documents *after* the complaint was unsealed."[96] *Frazier* suggests that in a *qui tam* case an attorney who receives such documents does not have an obligation to notify the opposing party that it has received the documents *while the case is under seal*, but it does have an obligation to seek a ruling from the court on what to do with the privileged documents while the case remains under seal and notify opposing counsel once the seal is lifted.

The court in *Frazier* awarded defendants the attorneys' fees and costs associated with the defendant's attempt to get its privileged documents back from relator's counsel, but did not find the facts presented warranted dismissal. It noted that the extraordinary circumstances of bad faith were not shown, particularly in light of the fact that *Qui Tam* Counsel kept the undisputed, privileged documents in a sealed box.[97] The defendant also sought sanctions against the relator personally, arguing that in addition to not having authorization to take the documents, his actions were contrary to the company's code of conduct that prohibited employees from disclosing confidential business information without authorization.[98] The court did not reach this issue because a settlement agreement on the separate motion for sanctions against the relator personally rendered the issue moot; but the court did find that that the relator "stole the documents" without permission.[99]

Using "its inherent powers, a district court may also sanction a party for wrongfully obtaining property or confidential information of an opposing party."[100] In *Glynn v. EDO Corp.*, a whistleblower (Glynn) was terminated after notifying a Department of Defense investigator about his concerns with technology his employer, Impact Science & Technology, Inc. ("IST"), was developing. After his termination, Glynn began communicating with a friend and current employee at IST who shared a "mutual distaste for IST management." The friend began sending internal IST documents and emails to Glynn and his counsel, including privileged communications. Once Glynn filed suit against IST alleging retaliation under the FCA, IST

continued on page 38

continued from page 37

counterclaimed against Glynn with a number of claims, including breach of contract. Although the court noted that its review of a handful of district court opinions outside of the Fourth Circuit suggested that dismissal or default judgment was warranted only in extreme circumstances that were not applicable in this case, it found that imposition of a $20,000 sanction against Glynn's counsel for improperly receiving internal IST documents (and asserting a common interest privilege in bad faith) was warranted.[101] Notably, the court did not find it necessary to address arguments from the parties as to whether the information was "proprietary, confidential, or protected by the attorney-client or work product privileges."[102] The court found it sufficient that "it was inappropriate…to surreptitiously acquire these internal IST documents outside of the normal discovery channels."[103]

– Counsel's Obligations to Protect Employee Privacy

Defense and in-house counsel face their own ethical challenges with respect to the privacy rights of third parties. Even while a case remains under seal, defense counsel may come to suspect that a potential whistleblower is employed in their midst. A common instinct may be to review a suspected whistleblower-employee's emails to determine whether that person is preparing or has already filed a *qui tam* complaint. From an ethical perspective, the risk is that the employer will come across privileged communications between the employee and his/her counsel. This context differs from the situations discussed above in that the documents are not obtained by a third party (inadvertently or otherwise), but rather are communicated through a medium that arguably makes the communication the employer's property. As a result, the ethical obligations to protect employee privacy hinge more on whether the argument can be successfully made that the comz-The crux of the attorney-client privilege is the protection of communications that are made in confidence between a client and an attorney for the purpose of obtaining legal advice. For the element of confidentiality to be met, the communication must be made with an intent that it be confidential and with the reasonable expectation that it will remain confidential.[104] Thus, the most effective tool for a company to thwart the creation of any privilege claim over its email is to design, implement, and publicize a strong computer monitoring policy. Such policies are considered a decisive factor in many court decisions which have rejected employee claims of privilege over work emails.

For example, in *Scott v. Beth Israel Medical Center*,[105] the court denied the plaintiff a protective order demanding that his employer return all emails sent to his lawyer on his work email that were obtained by his employers. The court found that the plaintiff could not have a reasonable expectation of privacy when he transmitted emails to his lawyer over the company's email system and therefore the documents were never protected by the attorney-client privilege.

The availability of the company's computer usage policy on the company's intranet and the language of the email usage policy were cited by the court as factors that were "critical to the outcome."[106] The usage policy made clear that it applied "to everyone who works at or for" the company and over an enumerated list of communication mediums, including "electronic mail systems."[107] In addition, the policy explicitly stated that "*employees have no personal privacy right in any material created, received, saved or sent using Medical Center communication or computer systems. The Medical Center reserves the right to access and disclose such material at any time without prior notice.*"[108] The court further found that notice of the policy need not be actual so long as the policy put the employee on constructive notice that the company retained the right to monitor all email.[109]

Other courts have agreed that employee email messages are not privileged where the employer provides effective notice that it monitors the use of its computer equipment, including emails that are created or stored on the company's equipment.[110] Some courts, however, have come to different conclusions, finding that emails may actually be privileged if the employee uses a personal email account from a third-party website, like Yahoo!, Gmail or Hotmail, as opposed to their work email.[111] Thus, defense counsel should be aware that some emails sent on a work computer may be deemed privileged, despite a corporate policy to the contrary. Even where a court finds that a robust email usage policy exists to negate an expectation of confidentiality, some email messages may still be protected if sent through personal email accounts. The risk that the privilege will be waived means that counsel for employees (*i.e.*, relators) would be prudent to advise their clients never to use work email (including personal accounts) to make privileged communications.

– Enforceability of Confidentiality Agreements

Companies are not without recourse if they fear confidential, proprietary, or potentially privileged documents were removed by an employee, particularly where a confidentiality agreement

exists in the employee's contract. Some courts have rejected employer claims of breach of confidentiality agreements, citing the policy argument that confidentiality agreements "cannot trump the FCA's strong policy of protecting whistleblowers who report fraud against the government."[112] But recent FCA decisions have rejected the notion that there should be a "public policy exception" that protects whistleblowers from civil liability claims for gathering documents as part of an investigation under the FCA.

In *U.S. ex rel. Cafasso v. Gen. Dynamics C4 Sys., Inc.*,[113] a whistleblower made a public policy argument after being counterclaimed by her former employer for breach of confidentiality agreement when she copied almost eleven gigabytes of data from company computers in anticipation of filing a *qui tam* action.[114] The district court granted summary judgment in favor of the defendants, reasoning that "public policy does not immunize Cafasso, [who] confuses protecting whistleblowers from retaliation for lawfully reporting fraud with immunizing whistleblowers for wrongful acts made in the course of looking for evidence of fraud."[115] The Ninth Circuit affirmed, concluding that "[s]tatutory incentives encouraging investigation of possible fraud under the FCA do not establish a public policy in favor of violating an employer's contractual confidentiality and non-disclosure rights."[116] Although the court noted there was "some merit" in the public policy exception proposed in certain instances, it did not decide the question, and instead noted that such an exception would not cover Cafasso's conduct, citing in particular the volume and scope of documents taken by Cafasso.[117] "An exception broad enough to protect the scope of Cafasso's massive document gather in this case would make all confidentiality agreements unenforceable as long as the employer later files a *qui tam* action."[118]

– *Obtaining an Employee Release Before the Qui Tam complaint is Filed*

Another mechanism through which companies often seek to protect themselves from *qui tam* complaints is to have the employee sign a broad release statement releasing all claims against the company at the end of the employment relationship. Courts have generally been reluctant to enforce an employee release that would bar the employee from bringing an FCA action, fearing that doing so would subvert the purpose of the *qui tam* provisions and the FCA itself.[119] More recent decisions, however, have begun to follow the so called "government knowledge rule" applied by the Fourth Circuit in *United States ex rel. Radcliffe v. Purdue Pharma*.[120] There, the court concluded that the release should be enforced because, unlike in earlier cases, the relator had it *after* the government knew about the fraudulent conduct underlying the relator's claims. The *Radcliffe* court "therefore agree[d] with the government that '[t]he proper focus of the inquiry is whether the allegations of fraud were sufficiently disclosed to the government.'"[121]

As with confidentiality agreements, the lessons learned from cases addressing the enforceability of employee release agreements are equally relevant to both defense and relator's counsel. Before signing a release (or relying on it), counsel should consider that the probability of it being enforceable is likely dependent on the following factors:

1. Whether the employee's claims have already been disclosed to the government (by the employee, the company, or by some other channel).
2. Whether the government had begun investigating the same underlying fraudulent conduct prior to the release being signed.
3. Whether the language of the release is broad enough to encompass a *qui tam* complaint.

For example, in *Radcliffe* the language releasing the relator's employer "from any and all liability" was considered broad enough to encompass the *qui tam* action that he filed after signing the release. A related issue which may arise is when an employer asks an employee to sign a statement or affidavit that the employee knows of no facts or information suggesting the company violated any law, including the FCA. Although such a statement may prove to be useful at trial, if the lawyer knows that the employee does, in fact, have information suggesting that the company violated a law, there is a risk that the lawyer could run afoul of Model Rule 8.4 by engaging in "conduct involving dishonesty, fraud, deceit or misrepresentation."

Conclusion

Because the majority of healthcare fraud cases involve the FCA and its *qui tam* provisions, lawyers representing healthcare organizations should be knowledgeable about the many ethical and legal issues and challenges that are particular to *qui tam* actions. Lawyers counseling corporations in FCA cases should also understand their professional duties to the client and non-client, like various corporate constituents, and be prepared to give advice that accounts for common conflict of interest and privilege considerations.

Robert Rhoad is a partner with Crowell & Moring LLP in Washington, D.C. He is a member of the firm's Healthcare and Government Contracts Groups and is Co-Leader of its Healthcare Litigation and False Claims Act Teams. Mr. Rhoad's practice is focused on defending companies and corporate executives facing criminal and/or civil government enforcement actions under the federal False Claims Act (including *qui tam* "whistleblower" actions), state false claims laws, and other fraud and abuse provisions. Prior to joining Crowell & Moring LLP in 2007, Mr. Rhoad spent nine years at a national law

continued on page 40

Ethical Issues Arising in Healthcare Fraud Investigations

continued from page 39

firm where he was a partner and Chair of its Healthcare Litigation Practice Group; prior to that, he served for nearly six years with the Navy Judge Advocate General's ("JAG") Corps. Mr. Rhoad, who currently serves as Co-Chair of the ABA Health Law Section's Ethics and Professionalism Committee and Vice-Chair of the Section's *ABA Health eSource* Editorial Board, has presented at numerous conferences and authored various articles on the False Claims Act and other areas related to fraud enforcement. Since 2002, he has taught litigation courses as an Adjunct Professor at The George Washington University Law School. Mr. Rhoad's full professional biography may be accessed at www.crowell.com/Professionals/Robert-Rhoad and he may be reached at *rrhoad@crowell.com*.

Endnotes

1 Section I of this article is abridged with permission from papers Mr. Rhoad co-authored with Andrew J. Demetriou, including *Ethical Issues in Managing Internal Investigations and Handling Pre-Unsealing Stages of False Claims Act Qui Tam Cases Involving the Health Care Industry*, presented at the ABA Health Law Section's 14th Annual Emerging Issues in Health Care Law Conference. Section II of this article is abridged with permission from a paper authored by firm colleagues Brian C. Elmer, Andy Liu, and Dalal Hasan, titled *Ethical and Legal Challenges in the Pre-Unsealing Stages of Qui Tam Litigation*, presented at the American Bar Association 2012 National Institute on the False Claims Act and *Qui Tam* Enforcement.

2 31 U.S.C. § 3729 *et seq.*

3 Press Release, U.S. Department of Justice, Department Recovers $3.8 Billion from False Claims Act Cases in Fiscal Year 2013 (Dec. 20, 2013), available at: www.justice.gov/opa/pr/2013/December/13-civ-1352.html.

4 The 1986 amendments expanded the FCA by, among other things, increasing the civil penalty imposed for each false claim, defining the knowledge element to include conduct performed with deliberate ignorance and reckless disregard, increasing the share that is received by *qui tam* relators, requiring the payment of the relator's reasonable attorneys' fees, allowing the Attorney General to issue civil investigative demands, and providing whistleblower protections to certain *qui tam* relators. P. Law 99-562, 100 Stat. 3153 (Oct. 27, 1986).

5 *Id.*

6 Pub. L. No. 111-21, 123 Stat. 1617.

7 Pub. L. 111-148, 124 Stat. 119. Amendments to PPACA were subsequently enacted shortly thereafter through the Health Care and Education Reconciliation Act of 2010, Pub. L. 111-152 ("HERA").

8 "First, Congress removed the requirement that the allegedly false claim actually be presented to the government for payment. Now liability may attach to claims that are submitted to a "contractor, grantee, or other recipient" of federal funds, regardless of whether a false claim was submitted to the government. Congress also removed the requirement that a subcontractor act with the specific intent "to get" a false claim paid "by the government." As a consequence, there is no longer a requirement that an individual or entity act with the specific intent to defraud the government." Robert T. Rhoad and Matthew T. Fornataro, "*A Gathering Storm: The New False Claims Act Amendments And Their Impact On Health Care Fraud Enforcement*," *The Health Lawyer*, Vol. 21, No. 6, at 14, (August 2009).

9 This article makes reference to the Model Rules of Professional Conduct ("Model Rules"), as adopted by the American Bar Association House of Delegates, which have largely been adopted by the states. Readers are cautioned to consult the local rules of jurisdictions in which they practice, for variations in the construct of the rules as well as the effect, if any, of the commentary included with the Model Rules. The Model Rules are available at:

www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html.

10 Model Rule 1.13(a).

11 Model Rule 1.13(a), cmt. [1].

12 *See* Model Rule 1.13(f) and cmt. [10].

13 *See* Model Rule 1.13(f) and cmt. [10].

14 *Id.*

15 Model Rule 1.7(a). The "consent" exceptions are in Model Rule 1.7(b).

16 Barry F. McNeil and Brad D. Brian, *Internal Corporate Investigations*, American Bar Association, pp. 212 (3d Ed. 2007).

17 Model Rule 1.7(b).

18 Barry F. McNeil and Brad D. Brian, *Internal Corporate Investigations*, American Bar Association, pp. 212 (3d Ed. 2007).

19 Model Rule 1.7 and cmt. [16].

20 Model Rule 1.7 and cmt. [18].

21 Model Rule 1.7 and cmt. [19].

22 Barry F. McNeil and Brad D. Brian, *Internal Corporate Investigations*, American Bar Association, pp. 213 (3d Ed. 2007).

23 Barry F. McNeil and Brad D. Brian, *Internal Corporate Investigations*, American Bar Association, pp. 215 (3d Ed. 2007).

24 Jones Day, Corporate Internal Investigations Best Practices, Pitfalls To Avoid, pp. 17-19 (2013).

25 Kimberly A. Dunne, Stuart C. Edmiston, and Patrick E. Kennell, *Weighing the Use of Individual Counsel in an Internal Investigation*, American Bar Association, White Collar Crime (2014).

26 *Id.* at L-12.

27 Stephen A. Saltzburg, *Ten Tips for Avoiding Problems in Internal Investigations*, American Bar Association, White Collar Crime (2014).

28 The latter name derives from the seminal case of *Upjohn Co. v. United States*, 449 U.S. 383 (1981).

29 *Miranda v. Arizona*, 384 U.S. 436 (1966).

30 Saltzburg, *Ten Tips for Avoiding Problems in Internal Investigations*, at K-4.

31 A reasoned discussion of these issues through the filter of attorney-client privilege considerations may be found in William W. Horton, *A Transactional Lawyer's Perspective on the Attorney-Client Privilege: A Jeremiad for* Upjohn, 61 BUS. LAW. 95 (2005).

32 *See, e.g.*, United States v. Nicholas, 606 F. Supp. 2d 1109 (C.D. Cal. 2009).

33 Courts in several states, notably Illinois, continue to utilize the control group test as to matters pending before state courts. *Upjohn* is binding precedent in federal court.

34 Edna Selan Epstein, *The Attorney-Client Privilege and the Work Product Doctrine*, pp. 143-45, American Bar Association (5th Ed. 2007).

35 *U.S. ex rel. Barko v. Kellogg Brown & Root, Inc.*, Case No. 1:05-CV-1276, 2014 WL 1016784 (D.D.C. Mar. 6, 2014).

36 2014 WL 1016784 at *3-4.

37 *In re Kellogg Brown & Root, Inc.*, 14-5055, 2014 WL 2895939 (D.C. Cir. June 27, 2014).

38 2014 WL 2895939 at *5.

39 *Id.* at *5.

40 *See generally* Jonathan Cone, Andy Liu, and Gail Zirkelbach, *How To Protect Internal Investigation Materials From Disclosure*, 56 Government Contractor ¶ 108 (Apr. 9, 2014).

41 Sean T. Carnathan, *Will The Company Cover An Ex-Officer's Legal Costs?*, ABA Business Law Section, Volume 13, Number 1 (September/October 2003) (quoting 8 Del. C. § 145(c)).

42 *See id* (citing 8 Del. C. § 145(a); *Waltuch v. Conticommodity Servs. Inc.*, 88 F.3d 87, 95 (2d Cir. 1996) (statute does not permit indemnification of officer who did not act in good faith). In criminal proceedings, the standard is whether the person "had reasonable cause to believe that the person's conduct was unlawful.")).

43 Barry F. McNeil and Brad D. Brian, *Internal Corporate Investigations*, American Bar Association, pp. 212 (3d Ed. 2007).

44 Pub. L. 107-204, 116 Stat. 745 (codified in scattered sections of 11, 15, 18, 28 and 29 U.S.C.).

45 For example, in its Sarbanes-Oxley-related rulemaking, the Securities and Exchange Commission required the national securities exchanges and Nasdaq to adopt listing standards requiring that listed company audit

committees have the authority to "engage independent counsel and other advisors" and that listed companies provide "appropriate funding, as determined by the audit committee," for such engagements. *See* 17 C.F.R. § 240.10A-3(b)(4) – (5).

46 In some circumstances, individual directors may even wish to involve their own personal counsel, in addition to any counsel otherwise advising the board or a committee thereof. This may be particularly likely where an individual director has joined the board after the events that gave rise to the investigation, or if an individual director otherwise feels that his or her interests may diverge from the interests of the majority of directors. Needless to say, interacting with such individual counsel may pose interesting political challenges for internal counsel. *See, e.g.,* Jones, *Call for Internal Probes Growing*, Nat'l L.J., Nov. 22, 2004, at 1, 7.

47 31 U.S.C. § 3730(b)(2)(2010).

48 American Bar Association Center for Professional Responsibility, *Ann. Model Rules of Prof'l Conduct* R. 3.1 (2011).

49 *Id.*, cmt. 1.

50 *Id.*

51 *Id.*

52 *Ann. Model Rules of Prof'l Conduct* R. 1.1.

53 *Id.*, cmt. 5.

54 *Mary Ann Pensiero, Inc. v. Lingle*, 847 F.2d 90, 94 (3d Cir. 1988).

55 Baicker-McKee, Steven, Federal Civil Rules Handbook, page 399 (2014) (quoting *ICU Medical, Inc. v. Alaris Medical Systems, Inc.*, 558 F.3d 1368, 1381 (Fed. Cir. 2009).

56 *Id.* at 399 (citing *Ledford v. Peeples*, 568 F.3d 1258, 1307 (11th Cir. 2009) (other citations omitted).

57 Fed. R. Civ. P. 11(c)(1).

58 28 U.S.C. §1927(2010).

59 31 U.S.C. § 3730(d)(4) (2010).

60 *See, e.g., U.S. ex rel. Ubl v IIF Data Solutions*, 650 F. 3d 445, 459 (4th Cir. 2011), citing *United States ex rel. Rafizadeh v. Continental Common, Inc.*, 553 F.3d 869, 875 (5th Cir. 2008) ("An action is not frivolous if existing law or a reasonable suggestion for its extension, modification, or reversal supports the action."); *Pfingston v. Ronan Eng'g Co.*, 284 F.3d 999, 1006 (9th Cir. 2002) ("An action is clearly frivolous when the result is obvious or the appellant's arguments of error are wholly without merit." (internal quotation marks omitted)); *Mikes v. Straus*, 274 F.3d 687, 705 (2d Cir. 2001) ("A claim is frivolous when, viewed objectively, it may be said to have no reasonable chance of success, and present no valid argument to modify present law."); *United States ex rel. Grynberg v. Praxair, Inc.*, 389 F.3d 1038, 1058 (10th Cir. 2004) ("[T]he plaintiff's action must be meritless in the sense that it is groundless or without foundation." (internal quotation marks omitted)).

61 *Pfingston v. Ronan Engineering Co.*, 284 F.3d 999, 1006 (9th Cir. 2002).

62 *See, e.g., United States ex rel. Mikes v. Straus*, 98 F. Supp. 2d 517, 529 (S.D.N.Y. 2000) (*qui tam* plaintiff's MRI claims were vexatious because they were "bereft of any objective factual support."); *United States ex rel. Bain v. Ga. Gulf Corp.*, 208 F. App'x 280 (5th Cir. 2006) (affirming district court's award of attorneys' fees to prevailing FCA defendant); *Pugach v. M&T Mortg. Corp.*, 564 F. Supp. 2d 153 (E.D.N.Y. 2008) (awarding prevailing FCA defendant $81,303.83 in attorneys' fees and $5,537.62 in costs); *United States ex rel. Cooper & Assocs., Inc. v. Bernard Hodes Grp., Inc.*, 422 F. Supp. 2d 225, 239 (D.D.C. 2006) (finding FCA defendant entitled to attorneys' fees when whistleblower "lodg[ed] claims that fly in the face of the available evidence").

63 *Alyeska Pipeline Serv. Co. v. Wilderness Soc'y,* 421 U.S. 240, 258-59 (1975) (internal quotations and citations omitted).

64 *See, e.g., United States ex rel. Branch Consultants v. Allstate Ins. Co.*, 560 F. 3d 371 (5th Cir. 2009).

65 *Id.* at 378. Courts are split on whether the later-filed action is barred permanently or only for so long as the first-filed action remains pending. Compare *United States ex rel. Carter v. Halliburton Co.*, 710 F.3d 171 (4th Cir. 2013) (first to file bar applies only so long as the first-filed action is still pending), with *United States ex rel. Shea v. Cellco P'Ship*, 2014 WL 1394687 (D.C. Cir. April 11, 2014) (first to file bar applies to related cases even if the first-filed action is no longer pending). The Supreme Court has granted a petition for certiorari in *Carter*, however, so the circuit split may soon be answered.

66 31 U.S.C. §§ 3730(b)-(c)(2010).

67 *Ann. Model Rules of Prof'l Conduct* R. 1.16(b) provides that, "[e]xcept as stated in paragraph (c), a lawyer may withdraw from representing a client if: (1) withdrawal can be accomplished without material adverse effect on the interests of the client, (2) the client persists in a course of action involving the lawyer's services that the lawyer reasonably believes is criminal or fraudulent; (3) the client has used the lawyer's services to perpetrate a crime or fraud; (4) the client insists upon taking action that the lawyer considers repugnant or with which the lawyer has a fundamental disagreement; (5) the client fails substantially to fulfill an obligation to the lawyer regarding the lawyer's services and has been given reasonable warning that the lawyer will withdraw unless the obligation is fulfilled; (6) the representation will result in an unreasonable financial burden on the lawyer or has been rendered unreasonably difficult by the client; or (7) other good cause for withdrawal exists."

68 *Ann. Model Rules of Prof'l Conduct* R. 1.16(c).

69 See *Ann. Model Rules of Prof'l Conduct* R. 1.2(c).

70 See Anthony L. Dewitt, *Is the Whistle Clean? An Examination of the Ethical Duties of Attorneys In Investigating and Pursuing False Claims Act Lawsuits*, 25 N. Ky. L. Rev. 715, 721 (Summer 1998).

71 *See, e.g., United States ex rel. Wildhirt v. AARS Forever, Inc.*, No. 09-c-1215, 2013 WL 5304092 (N.D. Ill Sept. 19, 2013) (denying relators' motion to dismiss counterclaims filed by defendants in False Claims Act case alleging relators had violated an employee confidentiality, non-compete and HIPAA agreement by taking and retaining confidential and HIPAA-covered records).

72 See *Ann. Model Rules of Prof'l Conduct* R. 4.2.

73 *Ann. Model Rules of Prof'l Conduct* R. 4.2, cmt. 8.

74 *Id.*

75 Notably, under Rule 4.2, cmt. 7, consent of the organization's lawyer is not required for communication with a *former* constituent, and if a constituent of the organization is represented in the matter by his or her own counsel, the consent by that counsel to a communication will be sufficient for purposes of the Rule. In some states, however, communications with certain former employees are treated the same way as communications with current employees.

76 36 False Cl. Act and *Qui Tam* Q. Rev. 13 (January 2005). The D.C. Rules of Professional Conduct are available at www.dcbar.org/bar-resources/legal-ethics/amended-rules.

77 D.C. Rule of Professional Conduct 4(b).

78 D.C. Rule of Professional Conduct 4(c).

79 *Ann. Model Rules of Prof'l Conduct* R. 4.2, cmt. 7 similarly specifies that in the case of a represented organization, the Rule would prohibit communications "with a constituent of the organization who supervises, directs or regularly consults with the organization's lawyer concerning the matter or has authority to obligate the organization with respect to the matter or whose act or omission in connection with the matter may be imputed to the organization… ."

80 *Ann. Model Rules of Prof'l Conduct* R. 4.2, cmt. 4.

81 *Ann. Model Rules of Prof'l Conduct* R. 8.4, cmt. 1.

82 *See, e.g., Glynn v. EDO Corp.*, JFM-07-01660, 2010 WL 3294347 (D. Md. Aug. 20, 2010)(citing *In re Shell Oil Refinery,* 143 F.R.D. at 108 ("PLC has not just communicated with a Shell employee, but has surreptitiously obtained from this employee proprietary documents belonging to Shell. Regardless of whether the PLC's communication with the Shell employee was in violation of [Louisiana's] Rule 4.2, the PLC's receipt of Shell's proprietary documents in this manner was inappropriate and contrary to fair play.... The PLC has effectively circumvented the discovery process and prevented Shell from being able to argue against production.")).

83 *Ann. Model Rules of Prof'l Conduct* R. 4.4, cmt. 1.

84 *Ann. Model Rules of Prof'l Conduct* R. 4.4(b) applies to receipt by a lawyer of *inadvertently* sent privileged materials and states, in pertinent part, "[a] lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender." *See* ABA Formal Op. 92-368, Inadvertent Disclosure of Confidential Materials, (Nov. 10, 1992) (withdrawn by ABA Formal Op. 04-437 Oct. 1, 2005).

85 ABA Formal Op. 94-382, *Unsolicited Receipt of Privileged or Confidential Materials*, (July 5, 1994).

86 ABA Formal Op. 06-440, *Unsolicited Receipt of Privileged or Confidential Materials: Withdrawal of Formal Opinion 94-382,* (May 13, 2006).

continued on page 42

Ethical Issues Arising in Healthcare Fraud Investigations

continued from page 41

87 ABA Formal Op. 11-460, Duty When Lawyer Receives Copies of Third Party's Email Communications With Counsel, (August 4, 2011).

88 *U.S. ex rel. Frazier v. IASIS Healthcare Corp.*, 2:05-CV-766-RCJ, 2012 WL 130332 (D. Ariz. Jan. 10, 2012).

89 *Id.* at *3.

90 *Id.* at *5.

91 *Id.* at *6-7.

92 *Id.* at *13.

93 *Id.* at *15 (citing Ariz. Ethics Op. No. 01-04 (Mar. 2001) at 5).

94 *Id.*

95 *Id.*

96 *Id.* (emphasis added).

97 *Id.*

98 *Id.* at *4.

99 *Id.* at *13.

100 *Glynn v. EDO Corp.*, JFM-07-01660, 2010 WL 3294347 (D. Md. Aug. 20, 2010) at *3 (internal citations omitted).

101 *Id.* at *3, *6. The court found that the misconduct in this case did not warrant the extraordinary sanction of dismissal or default because (1) IST had not proven that it was or would be sufficiently prejudiced "to trump the important public policy of resolving the claims at issue on the merits," "any documents that were in fact helpful to Glynn would have been disclosed in discovery anyway," and, to the extent that privileged information was obtained that would not have been revealed through discovery, IST had not explained how it would be prejudiced; (2) the degree of culpability of Glynn and his lawyers was substantially less than in most cases where dismissal was imposed, particularly because IST had not presented conclusive evidence that Glynn or his lawyers "expressly requested" that the documents be acquired and handed over.

102 *Id.* at *5.

103 *Id.* (citations omitted).

104 See John K. Villa, *Emails Between Employers and Their Attorneys Using Company Computers: Are they Still Privileged?*, 26 No. 3 ACC Docket 102, 103 (2008) (citing *Long v. Marubeni American Corp.*, No. 05-CV-639, 2006 WL 2998671, at *3 (S.D.N.Y. Oct. 19, 2006) ("Confidentiality is an aspect of a communication that must be shown to exist to bring the communication within the attorney-client privilege.")).

105 *Scott v. Beth Israel Med. Ctr. Inc.*, 847 N.Y.S.2d 436 (Sup. Ct. 2007).

106 *Id.* at 441.

107 *Id.* at 439.

108 *Id.* (emphasis added).

109 *Id.* at 440.

110 *See, e.g., Kaufman v. Sungard Inv. Sys.*, No. 05-CV-1236, 2006 WL 1307882 (D.N.J. May 10, 2006); *Sims v. Lakeside School*, No. C06-1412, 2007 WL 2745367 (W.D. Wash. Sept. 20, 2007); *Banks v. Mario Indus. Of Va., Inc.*, 650 S.E.2d 687 (Va. 2007).

111 *See, e.g., Curto v. Medical Communications, Inc.*, No. 03-CV-632, 2006 WL 1318387 (E.D.N.Y. May 15, 2006).

112 *U.S. v. Cancer Treatment Centers of America*, 350 F. Supp. 2d 765, 773 (N.D. Ill. 2004).

113 *U.S. ex rel. Cafasso v. Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047 (9th Cir. 2011).

114 *Id.* at 1062.

115 *U.S. ex rel. Cafasso v. Gen. Dynamics C4 Sys. Inc., 2009 WL 1457036*, *13 (D. Ariz. May 21, 2009).

116 637 F.3d 1047 at 1062.

117 *Id.*

118 *Id.*

119 *See, e.g., United States ex rel. Green v. Northrop Corp.*, 59 F.3d 953, 963 (9th Cir. 1995) (refusing to enforce employee release, reasoning that allowing a relator to forfeit the right to bring a *qui tam* action would "threaten to nullify the incentives" that Congress had added to the Act, namely to bring fraud allegations to the attention to the government that they had no knowledge of).

120 600 F.3d 319 (4th Cir. 2010).

121 *Id.* (citation omitted).

Gathering Evidence in Qui Tam Actions[1]

By: Joel M. Androphy[1], Sarah Frazier, and Rachel Grier

Qui tam whistleblowers first discover fraud against the government in a variety of different ways; some learn it from a business owner's own statements while others witness it in caring for a patient who has patently not received a billed-for treatment. Documentary evidence does not always accompany that first discovery of fraud, but without it, a case brought under the False Claims Act can devolve into a swearing match, as the government, relators' counsel, and most whistleblowers are keenly aware. Consequently, even after making the difficult decision to blow the whistle on an employer by reporting FCA violations, a soon-to-be *qui tam* relator must often gather evidence to support his or her allegations. Although the FCA encourages citizens to investigate and gather evidence to prove a fraud, a tension exists between the interests of the public, the government, and the relator on the one hand, and the defendant's interest in protecting its property, including potential proprietary information, on the other. A potential whistleblower may well ask: How much evidence must I muster to support a *qui tam* action? What ethical concerns or legal consequences exist when I gather documents and other evidence from an employer?

These questions should not intimidate or prevent a potential relator from reporting fraud against the government. Generally, a potential relator may gather anything in his or her care, custody, or control that evidences fraud covered by the FCA.

The Relator Has a Duty to Gather Evidence.

Upon filing a *qui tam* action, a relator *must* voluntarily provide the government with a "copy of the complaint and written disclosure of substantially *all material evidence and information* the person possesses" regarding the allegations.[2] The more relevant evidence the relator can provide to his or her attorney and the government, the more likely the relator will be able to substantiate the allegations and ultimately succeed in prosecuting the lawsuit.

Section 3730(h) of the FCA protects potential relators from retaliation for "lawful acts done . . . in furtherance of an action under this section, including investigation."[3] Employers often flout the FCA's "protected activity" provision and terminate whistleblowers under a pretext. Nevertheless, this section of the FCA "manifests Congress' intent to protect employees while they are collecting information about a possible fraud, *before* they have put all the pieces of the puzzle together."[4]

Indeed, the relator needs this Protection even after the case is filed because he or she faces special pleading hurdles that apply to fraud cases under Federal Rule of Civil Procedure 9(b),[5] yet is not provided access to formal discovery beforehand while the case is under seal. Although the government has access to certain tools of discovery during the seal period, it nevertheless relies heavily on relators and their counsel to investigate the fraud allegations while the case is under seal, and in particular, to provide it with documentary evidence.[6] In its brief in *U.S. ex rel. Grandeau v. Cancer Treatment Centers of America*, the government emphasized the importance of a relator's ability to provide documents to the government:

[I]n order to proceed with an FCA action, the FCA requires that relators disclose to the United States alone "substantially all material evidence and information the person possesses," 31 U.S.C. § 3730(b)(2), and ties relator's share to the importance of her participation in the action and the relevance of the information she provided. . . . Not only does the FCA contemplate that relators will share evidence with the government, but also that they will do so in secrecy.[7]

An important reason for such reliance is the risk that a defendant, once asked for a particular document, will respond, truly or falsely, that the document is lost, misplaced, or destroyed in the normal course of business.

The Interests in Disclosure of Potentially Relevant Evidence within a Relator's Care, Custody, or Control Outweigh a Defendant's Attempt to Privatize Fraudulent Activity.

Although gathering evidence creates a direct conflict between competing interests, the interest in disclosing the fraud generally outweighs the defendant's interest in privatizing the fraud. "Implicit in the very purpose of the statute is an assumption that individuals who become *qui tam* relators possess and are willing to disclose to the government inside evidence of fraud – whether in the form of documents or other information—that their employers or other potential FCA defendants would rather that relators not disclose to the government."[8] From the defendant's perspective, the employee's duties of loyalty and confidentiality trump all other interests, and any breach is intolerable. As a result, after an employee gathers and discloses the evidence of fraud, employers often file counterclaims against relators for breach of confidentiality agreements, breach of fiduciary duty, and conversion.[9] In ruling on these counterclaims, courts consider several factors, including (1) whether the relator had access to the documents in the course and scope of employment, (2) the relevancy of the documents, and (3) the applicability of a valid privilege or enforceability of a confidentiality agreement.

First, the relator must have "legitimate possession and custody of the documents."[10] For example, relators may gather and produce to the government voluminous documents, e-mails, and other communications received during the course of their employment. As long as the relator is preparing to file a *qui tam* suit or otherwise disclose the information to the government, his search efforts should be unimpaired. A relator may

not, however, rummage through someone's office without permission or gain computer access unlawfully or through false pretenses.

Second, courts consider the relevance of the documents at issue. *Qui tam* cases typically involve hundreds of thousands, sometimes millions, of documents. Therefore, relators who have no prior *qui tam* experience should not have the burden of analyzing the legal significance of each document before gathering and preserving for their *qui tam* counsel to review—a process that often consumes a significant amount of counsel's time.[11] So long as the relator has some basis to reasonably believe that the documents have some relevance to the allegations, collection of such documents should be permitted.

Finally, equally important in ruling on a defendant's counterclaims are privilege or confidentiality concerns. A defendant may attempt to exclude certain evidence gathered by a relator by asserting that the evidence is privileged. Depending on the evidence at issue, a relator may challenge the defendant's assertion of privilege. For example, a relator may contradict a defendant's claim that a document is protected by the attorney-client privilege by arguing that under the crime-fraud exception, "communications made for an unlawful purpose or to further an illegal scheme are not privileged."[12]

Courts have noted that employee confidentiality agreements tend to tie relators' hands unacceptably in the disclosure of relevant evidence and prohibit relators from carrying out legitimate investigations that are encouraged by public policy. The Supreme Court has held that a private contract is "unenforceable if the interest in its enforcement is outweighed in the circumstances by a public policy harmed by enforcement of the agreement."[13] The government has taken the position that "[a] private agreement that broadly prevents a relator from turning over any non-privileged evidence of fraud which she 'possesses' to the Government should not be enforced" because such "broad corporate confidentiality agreements would frustrate the purposes of the FCA by proscribing the relator from providing the Government with some of the best evidence of fraud, gleaned from the company's files."[14] Defendants' confidentiality agreements are thus unenforceable to the extent that they conflict with the purpose of the FCA and prevent relators from disclosing non-privileged information evidencing fraud.[15]

In *U.S. ex rel. Head v. Kane Co.*, the court held that a relator did not breach a separation agreement by failing to return an e-mail containing direct evidence of the defendant's fraud.[16] The court reasoned that enforcing a private agreement that requires a *qui tam* plaintiff to turn over to the defendant who is under investigation the only copy of a document that is likely to be needed as evidence at trial would unduly frustrate the purpose of Section 3730(b)(2), which requires relators to provide the government with "all material evidence and information the person possesses" regarding the fraud allegations.[17]

Practically speaking, concerns regarding confidentiality, trade secrets, and proprietary information need not impede disclosure, as the Protections and requirements governing disclosure in the FCA involve and allow only disclosure *to the government*. The seal protects the defendant from disclosure to competitors and others initially, and a protective agreement can limit unnecessary disclosure once the seal is lifted.

Conclusion

The FCA, as the primary tool for combating fraud and recovering funds fraudulently obtained from the government, should be interpreted in a manner that encourages whistleblowers to come forward. Courts should, and generally do, allow relators significant leeway when gathering evidence because relators are unofficial agents of law enforcement and because evidence of fraud could be lost, misplaced, or suppressed if relators do not retrieve it. The public's interests are best served by affording relators Protections that acknowledge their efforts and personal sacrifices they make during their investigations.

1. Author of treatise, Federal False Claims Act and Qui Tam Litigation, Law Journal Press (2010), research source of the issues discussed in this article.
2. 31 U.S.C. § 3730(b)(2) (emphasis added).
3. 31 U.S.C. § 3730(h).
   U.S. ex rel. Yesudian v. Howard Univ., 153 F.3d 731, 740 (D.C. Cir. 1998) (emphasis in original); *see Thompson v. Quorum Health Res., LLC*, 2009 WL 4758752 (W.D. Ky. Dec. 7, 2009) (concluding the plaintiff's good faith while gathering documents related to his fraud allegations and speaking with his attorney about his potential *qui tam* satisfied the requirement to engage in protected activity).
4. Federal Rule of Civil Procedure 9(b) requires that allegations of fraud be pled with particularity. *See* Fed. R. Civ. P. 9(b).
5. *See* Robert Fabrikant, *In the Shadow of The False Claims Act: "Outsourcing" the Investigation by Government Counsel to Relator Counsel During the Seal Period*, 83 N.D. L. Rev. 834, 843 (2007) ("[D]uring the seal period, relator's counsel, at the request of the government, conducts factual and legal research [and] participates in interviewing fact witnesses."); *see also Dep't of Justice Relator's Share Guidelines* (Dec. 10, 1996), *available at* http://www.taf.org/publications/PDF/oct97.pdf (last visited June 7, 2011) (noting as item for consideration in determining relator's share in the recovery, "The relator provided substantial assistance during the investigation and/or pretrial phase of the case.").
6. Submission of the United States as Amicus Curiae in Support of Relator's Motion to Dismiss the Counterclaims of Defendant Midwestern Regional Medical Center, Inc. at 7, *U.S. ex rel. Grandeau v. Cancer Treatment Ctrs. of Am.*, 99-C-8287 (E.D. Ill. Apr. 2, 2004).
7. Submission of the United States as Amicus Curiae in Support of Relator's Motion to Dismiss the Counterclaims of Defendant Midwestern Regional Medical Center, Inc. at 7, *U.S. ex rel. Grandeau v. Cancer Treatment Ctrs. of Am.*, 99-C-8287 (E.D. Ill. Apr. 2, 2004).
8. *See, e.g., U.S. ex rel. Grandeau v. Cancer Treatment Ctrs. of Am.*, 350 F. Supp. 2d 765, 772-74 (N.D. Ill. 2004).
9. Submission of the United States as Amicus Curiae in Support of Relator's Motion to Dismiss the Counterclaims of Defendant Midwestern Regional Medical Center, Inc. at 16, *U.S. ex rel. Grandeau v. Cancer Treatment Ctrs. of Am.*, 99-C-8287 (E.D. Ill. Apr. 2, 2004).

10. *But see U.S. ex rel. Cafasso v. General Dynamics C4 Sys., Inc.*, CV 06-1381-PHX-NVW, 2009 WL 3723087, at *5-7 (D. Ariz. Nov. 4, 2009) (concluding that the relator indiscriminately gathered documents wholesale without regard to the documents' relevancy to the *qui tam* action). *Cafassso* is an outlier case and is not the majority rule on gathering evidence in *qui tam* cases.
11. *See, e.g., U.S. ex rel. Smart v. CHRISTUS Health*, CIV A C-05-287, 2009 WL 1658008, at *5 (S.D. Tex. June 12, 2009) (concluding that relator failed to meet his burden of showing that the crime-fraud exception applies because relator's brief does not identify where in the complaint or the attachments in particular the court was to find the evidence on which to base a prima facie case that defendants' attorneys furthered a fraud).
12. *Town of Newton v. Rumery*, 480 U.S. 386, 392 (1987); *see* Restatement (Second) of Agency § 395 cmt. F (1958) ("An agent is privileged to reveal information confidentially acquired by him in the course of his agency in the Protection of a superior interest of himself or of a third person," where, for example, "the confidential information is to the effect that the principal is committing or is about to commit a crime.").
13. Brief for United States as Amicus Curiae in Support of the Appellee at 25-26, *U.S. ex rel. Cafasso v. General Dynamics C4 Sys., Inc.*, 09-16181 (9th Cir. May 5, 2010).
14. *See, e.g., U.S. ex rel. Grandeau v. Cancer Treatment Ctrs. of Am.*, 350 F. Supp. 2d 765, 773 (N.D. Ill. 2004) ("[T]he confidentiality agreement cannot trump the FCA's strong policy of protecting whistleblowers who report fraud against the government."); *X Corp. v. John Doe*, 805 F. Supp. 1298, 1310 n.24 (E.D. Va. 1992) (noting that an agreement would be void as against public policy if it would prevent "disclosure of evidence of a fraud on the government").
15. 668 F. Supp. 2d 146, 151-52 (D.D.C. 2009).
16. *See id.* at 152.

The Intersection of the Dodd-Frank Act and the Foreign Corrupt Practices Act: What All Practitioners, Whistleblowers, Defendants, and Corporations Need to Know

Vol. 59, The Advocate: Litigation Section of the State Bar of Texas, Summer 2012

By: Joel M. Androphy[1] and Kathryn Nelson

I. Introduction

With the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), government authorities are no longer the only ones with a monetary interest in ferreting out those who violate federal laws. Specifically, Section 922 of the Dodd-Frank Act provides a whistleblower program that rewards individuals who assist the Securities and Exchange Commission (SEC) in uncovering securities violations, including Foreign Corrupt Practices Act (FCPA) violations. Because the Dodd-Frank Act allows individual whistleblowers to reap significant benefits by reporting offenders and because the SEC and Department of Justice (DOJ) have increased FCPA prosecutions in recent years, global companies and their employees, especially those in the pharmaceutical and medical device industry, should understand how the Dodd-Frank Act and the FCPA intersect.

II. The Dodd-Frank Act and the SEC Whistleblower Program

A. Overview of the SEC Whistleblower Program

The SEC's whistleblower program was implemented under Section 922 of the Dodd-Frank Act and is primarily intended to reward individuals who provide original information to the SEC that leads to a successful enforcement action. Dodd-Frank also prohibits retaliation by employers against individuals who provide the SEC with information about possible securities violations.

In passing the Dodd-Frank Act, Congress substantially expanded the agency's authority to compensate individuals who provide the SEC with information about violations of the federal securities laws. Under Dodd-Frank, awards can now be up to thirty (30) percent of the monetary sanctions or recovery obtained by the SEC.

B. Requirements of a SEC Whistleblower

Under the SEC whistleblower program, a whistleblower must: (1) voluntarily provide the SEC, (2) with original information that (3) leads to the successful enforcement by the SEC of a federal court or administrative action, (4) in which the SEC obtains monetary sanctions totaling more than $1 million. Each of these requirements is explained in turn:

1. A whistleblower is deemed to have provided information voluntarily if the whistleblower has provided information before the government, a self-regulatory organization or the Public Company Accounting Oversight Board asks for it directly from the whistleblower or the whistleblower's representative.
2. Original information must be based upon the whistleblower's independent knowledge or independent analysis, not already known to the Commission and not derived exclusively from certain public sources.
3. A whistleblower's information can be deemed to have led to a successful enforcement action if: (1) the information is sufficiently specific, credible and timely to cause the SEC to open a new examination or investigation, reopen a closed investigation, or open a new line inquiry in an existing examination or investigation; (2) the conduct was already under investigation when the information was submitted, and the information significantly contributed to the success of the action; or (3) the whistleblower reports original information through his or her employer's internal whistleblower, legal, or compliance procedures before or at the same time it is passed along to the SEC; the employer provides the whistleblower's information (and any subsequently-discovered information) to the SEC; and the employer's report satisfies prongs (1) or (2) above.
4. With regard to the $1 million requirement, the rules permit aggregation of multiple SEC cases that arise out of a common nucleus of operative facts as a single action. These may include proceedings involving the same or similar parties, factual allegations, alleged violations of the federal securities laws, or transactions or occurrences.

C. Excluded as SEC Whistleblowers

Under the SEC Whistleblower program, certain people generally will not be considered for whistleblower awards, including:

- People who have a pre-existing legal or contractual duty to report their information to the Commission;
- Attorneys (including in-house counsel) who attempt to use information obtained from client engagements to make whistleblower claims for themselves (unless disclosure of the information is permitted under SEC rules or state bar rules);
- People who obtain the information by means or in a manner that is determined by a U.S. court to violate federal or state criminal law;
- Foreign government officials;
- Officers, directors, trustees or partners of an entity who are informed by another person (such as by an employee) of allegations of misconduct, or who learn the information in connection with the entity's processes for identifying, reporting and addressing possible violations of law (such as through the company hotline).
- Compliance and internal audit personnel; and
- Public accountants working on SEC engagements, if the information relates to violations by the engagement client.

However, under certain circumstances, compliance and internal audit personnel, as well as public accountants, can become whistleblowers when: (1) the whistleblower believes

disclosure may prevent substantial injury to the financial interest or property of the entity or investors; (2); the whistleblower believes that the entity is engaging in conduct that will impede an investigation; or (3) at least 120 days have elapsed since the whistleblower reported the information to his or her supervisor or the entity's audit committee, chief legal officer, chief compliance officer—or at least 120 days have elapsed since the whistleblower received the information, if the whistleblower received it under circumstances indicating that these people are already aware of the information.

Certain other people, such as employees of certain agencies and persons who are criminally convicted in connection with the conduct, are already excluded by Dodd-Frank. In order to prevent wrongdoers from benefiting by, in effect, blowing the whistle on themselves, the rules do not allow the SEC to pay a culpable whistleblower an award that is based on either: (1) the monetary sanctions that such culpable individuals themselves pay in the resulting SEC action, or (2) the monetary sanctions paid by entities whose liability is based substantially on conduct that the whistleblower directed, planned or initiated.

III. Foreign Corrupt Practices Act

The Dodd-Frank Act's SEC whistleblower program offers substantial rewards to individuals for assisting the SEC in uncovering FCPA violations. Because the number of FCPA investigations has increased, international companies and their employees need to understand the FCPA and how to deter FCPA violations.

A. Overview of the FCPA

The FCPA subjects U.S. citizens and issuers to criminal liability for payments to foreign officials in order to secure business.[2]Although certain foreign countries have laws similar to the FCPA, the SEC and the DOJ's ability to enforce the FCPA,[3] civilly and criminally only extends to American companies and citizens who bribe foreign officials, not the foreign officials who are the bribe recipients—an aspect of the law that causes Americans to be on an uneven playing field in terms of competitive advantages.[4] To prove a violation of the FCPA's anti-bribery provisions, the government must prove the following eight elements:

1. The defendant was a "domestic concern" or an officer, director, employee, or agent of a "domestic concern"[5] or an "issuer" or an officer, director, employee, or agent of such issuer or any stockholder thereof acting on behalf of such issuer;[6]
2. The defendant with respect to the charged conduct specifically intended to make use of the mails or means of interstate commerce;[7]
3. The defendant acted corruptly and willfully;
4. The defendant specifically intended to act in furtherance of a payment—or an offer, promise or authorization for payment—or an offer, gift, promise to give or authorization of the giving of anything of value;
5. The recipients of the payments were "foreign officials;"[8]
6. The defendant knew that all or a portion of the payment was to be offered, given, or promised, directly or indirectly, to a foreign official;

7. The payment was specifically intended to be for one of three purposes: (1) to influence an act or decision of the foreign public official in his or her official capacity; (2) to induce the foreign public official to do or omit to do any act in violation of that official's lawful duty; or (3) to induce that foreign official to use his or her influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality; and
8. The payment was specifically intended to obtain or retain business for or with, or directing business to, any person.

B. Issues and Ambiguities in FCPA Elements

With the increased number of prosecutions under the FCPA, some of its terms and provisions have received criticism, including the definitions and interpretations of "corruptly and willfully," "knowingly," and "foreign official."

1. Corruptly and Willfully

In prosecuting a defendant for an FCPA violation, the government must prove that the defendant acted both corruptly and willfully. A person acts "corruptly" if he acts voluntarily and intentionally, with a bad, wrongful, or improper purpose or evil motive and a specific intent to influence a foreign official to misuse his or her official position to achieve an unlawful result, or a lawful result by some unlawful method or means.[9]

And a person acts "willfully" if he acts deliberately and with the specific intent to do something that the Unites States laws forbid, that is, with a bad purpose to disobey or disregard the law. In other words, the government must prove that the defendant acted with knowledge that his conduct violated United States laws.[10] The defendant must believe the transaction was illegal. He cannot be convicted of being negligent or mistaken—more is required than that.[11]

Proving that a defendant acted both corruptly and willfully requires the government to prove that the defendant knew his actions violated the FCPA—a difficult burden if the defendant never received FCPA training.

2. Foreign Official

Another issue at the center of FCPA prosecutions is the FCPA's definition of "foreign official." The FCPA defines "foreign official" as "any officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization."[12] But the FCPA does not define "instrumentality."[13]

Without defining who is an instrumentality of a foreign official, the government has expanded the definition to cover employees not intended to be covered either under the text of the FCPA or the underlying purpose of the FCPA. For example, the government has recently taken the position that all employees of a government-owned foreign entity

are "foreign officials" within the meaning of the statute because the word "instrumentality" in the definition of foreign official includes state-owned or state-controlled foreign entities. Recent FCPA litigation has focused on whether the definition of "instrumentality" includes foreign state-owned entities and their employees.[14]

3. Knowingly

An additional hurdle that the government must overcome in an FCPA prosecution is proving that the defendant *knew* that the intended recipient of a payment was a foreign official.[15]

American employees and corporations often conduct business in a foreign country with foreign state-owned and state-controlled companies without knowing that the U.S. government will later contend that the employees of these companies are foreign officials. As noted above, whether a person is a foreign official is ambiguous because the statute itself fails to provide adequate guidance on this term, and therefore, proving that a defendant *knew* that a certain employee was a foreign official is a significant burden for the government.

B. Statutory Exception and Defenses

In addition to using the above-mentioned ambiguities and issues to defend against an FCPA prosecution, the FCPA expressly provides a statutory exception and two affirmative defenses.

1. Exception

Under the FCPA's exception, payments are not in violation of the FCPA if the payments were facilitating or expediting payments to a foreign official "the purpose of which is to expedite or to secure the performance of a routine governmental action"—a defined term under the FCPA.[16] This exception to the FCPA is commonly referred to as the "grease payment" exception.

2. Affirmative Defenses

The FCPA sets forth two affirmative defenses: (1) the payments, while a violation of the FCPA, were legal under the written laws of the foreign country, and therefore, defendant should not be convicted of the charges in the indictment;[17] (2) the payment, gift, offer, or promise of anything of value that was made, while a violation of the FCPA, was a reasonable and bona fide expenditure.[18]

IV. Enforcement Trends in FCPA Healthcare Cases

In recent years, FCPA enforcement activity by the SEC and the DOJ has increased sharply. For example, in 2000, the government did not prosecute a single FCPA case, but in 2010, the DOJ's Criminal Division imposed $1 billion in penalties in FCPA cases—the largest in the history of FCPA enforcement.[19]

In the pharmaceutical and medical device industry, American companies are often at an increased risk of FCPA liability because many companies conduct business in foreign countries that have national healthcare systems. These national healthcare systems have publicly-owned and operated hospitals whose health care providers are government employees providing health care services in their official capacities. According to the U.S. government's interpretation of the FCPA, these employees are foreign officials under the FCPA.

Examples of potential FCPA violations include American pharmaceutical companies and their employees paying doctors and health officials abroad to encourage those individuals to order or prescribe their products or paying foreign doctors to oversee clinical trials of drugs and devices. These payments draw the attention of the U.S. government, and if these payments are made to persons who qualify as "foreign officials" under the FCPA, the pharmaceutical company may face civil or criminal charges in the United States.

In a speech on November 17, 2009 at the 22nd National Forum on the Foreign Corrupt Practices Act, Lanny A. Breuer, the Assistant Attorney General for the DOJ's criminal division, commented on how the nature of the pharmaceutical industry itself exposes American companies to FCPA liability:

In some foreign countries and under certain circumstances, nearly every aspect of the approval, manufacture, import, export, pricing, sale and marketing of a drug product may involve a 'foreign official' within the meaning of the FCPA. The depth of government involvement in foreign health systems, combined with fierce industry competition and the closed nature of many public formularies, creates, in our view, a significant risk that corrupt payments will infect the process.[20]

The potential prosecution of pharmaceutical companies should influence these companies' marketing strategies abroad, and company executives should insist that their foreign subsidiaries not pay bribes to foreign health officials or doctors.

As many international pharmaceutical companies have already discovered, the DOJ and SEC have been increasing the number FCPA investigations by examining the entire pharmaceutical and medical device industry.[21] For example, the SEC and DOJ have reportedly investigated AstraZeneca, Lilly Eli & Co., Johnson & Johnson, Medtronic, Merck, and Zimmer; and other companies, including Novo Nordisk and Syncor, have already paid substantial fines for violations of the FCPA.[22] Given the international nature of the industry, pharmaceutical and medical device companies need to be prepared to face FCPA investigations by the DOJ and SEC.

V. Considerations for all Corporate Defendants, Individual Defendants, Whistleblowers, and their Counsel

A. Corporate Defendant's Perspective

Companies that violate the FCPA pay significant fines and penalties, often willingly as a risk-based decision, with the understanding that these sanctions are part of the cost of

doing business in foreign countries. The government's primary resolution vehicles for FCPA enforcement actions are plea agreements, deferred prosecution agreements (DPAs), and non-prosecution agreements (NPAs). Rather than endure a lengthy, expensive trial and potentially suffer harm to their business and goodwill, many companies prefer to enter plea agreements, DPAs, and NPAs.[23] Before signing any agreement with the government, companies should be aware that such agreements often require the company to implement a compliance monitoring program, waive the attorney-client privilege, turnover employees' private documents and data, cut off support for certain employees' legal defense, and terminate the employment of those who do not cooperate with government investigations.

Another arrow in the government's quiver is debarment from participation in federal and state health care programs. Under 42 U.S.C. § 1320A-7, the government has the authority to debar or exclude entities from participation in Medicare and State Health Care Programs.[24] All the disadvantages of plea agreements, DPAs, and NPAs pale in comparison to debarment from participation in these government programs. But as a practical matter, the government rarely imposes this devastating sanction in part because certain companies that bribe foreign officials also do extensive business with various U.S. agencies under government contracts; thus, debarment for these companies penalizes not only the companies, but also the government agency with which they does business.[25]

Knowing all the consequences that accompany FCPA litigation, many companies choose to be proactive and self report to the DOJ and SEC to take advantage of any leniency that the government might offer. Because a company is often held to a strict liability standard for the acts of its employees, a company should take steps to lessen the probability that it will violate the FCPA. For example, all companies should consider the following preventative measures:

- Train employees on the FCPA and the consequences for U.S. citizens doing business abroad who violate the FCPA's anti-bribery provisions by bribing foreign officials.
- Educate employees on the cultural differences in the countries in which the company conducts business.
- Caution employees to be mindful of who might be considered a foreign official in third world countries because the government often has extensive "ownership" and "control" over all economic activities, and in recent FCPA actions, the U.S. government has considered employees of state-owned foreign entities to be foreign officials under the FCPA.
- Implement an FCPA compliance program, a code of conduct, and specific policies and procedures regarding conducting business in foreign countries.
- Incorporate provisions into contracts with intermediaries setting forth strict guidelines on their interaction with foreign government officials and prohibitions on acts that would violate the FCPA.
- Provide resources and procedures for employees to report FCPA violations or meet with general counsel to address questionable foreign business practices that might violate the FCPA.

- Request an opinion from the Attorney General under 15 U.S.C. § 78dd-2(f) to determine whether prospective conduct would violate the FCPA.
- Consider the advantages of self-reporting through voluntary disclosures to the SEC and DOJ if internal investigations reveal violations of the FCPA.

B. Individual Defendant's Perspective

FCPA prosecutions of individuals are not a prevalent as corporate prosecutions. Individuals charged with FCPA violations more likely than not worked at companies that failed to take precautionary measures, implement FCPA policies and procedures, or provide FCPA training. But unlike the companies for which they worked, individuals do not have deep pockets to pay FCPA sanctions. Consequently, many FCPA defendants plead guilty without a fight to avoid the possibility of being sent to prison.

As long as FCPA defendants—both individuals and corporations—enter into plea agreements, DPAs, and NPAs, the government will continue to build its arsenal of "prosecutorial common law" to support its aggressive and slanted interpretation of the FCPA.[26] Court acceptance of plea agreements does not convert the government's pronunciations on the law into sources of legal authority. Indeed, the government's strategy of creating its own would-be common law threatens to strip the federal courts of their judicial power to interpret the FCPA. The federal courts, and not the Department of Justice nor any other division of the executive branch, are the final arbiters of what the FCPA actually provides.[27]

Obstacles in defending an FCPA action that are common to both individual defendants and corporate defendants include obtaining records from foreign countries, hiring experts on foreign law, and gathering related opinions from foreign courts or government agencies regarding the alleged conduct. Given the adversities associated with defending an FCPA case, for many individuals, the process is cost-prohibitive.

C. Whistleblower's Perspective

Much like the False Claims Act (and to a lesser extent the IRS whistleblower program),[28] the SEC's whistleblower program may foster an environment that will lead to more individuals coming forward as whistleblowers. The SEC whistleblower provisions describe the procedures for submitting information to the SEC and for making a claim for an award after an action is brought. The claim procedures provide opportunities for whistleblowers to present their claim before the SEC makes a final award determination. Under the provisions, the SEC also will pay an award based on amounts collected in related actions brought by certain agencies that are based upon the same original information that led to a successful SEC action.

Regarding the increased anti-retaliation provisions, a whistleblower who provides information to the SEC is protected from employment retaliation if the whistleblower possesses a reasonable belief that the information he or she is providing relates to a possible securities law violation that has occurred, is ongoing, or is about to occur. In addition, the rules make it unlawful for anyone to interfere with a whistleblower's efforts to communicate with the SEC, including threatening to enforce a confidentiality agreement.

Although the SEC's whistleblower provisions do not require that employee whistleblowers report violations internally in order to qualify for an award, the rules strengthen incentives that had been proposed and add certain additional incentives intended to encourage employees to use their own company's internal compliance programs when appropriate to do so. For example, the rules make a whistleblower eligible for an award if the whistleblower reports internally and the company informs the SEC about the violations. In addition, an employee is considered a whistleblower under the SEC program as of the date that the employee reports the information internally—as long as the employee provides the same information to the SEC within 120 days.

Through this provision, employees are able to report their information internally first while preserving their "place in line" for a possible award from the SEC. More importantly, the rules provide that a whistleblower's voluntary participation in a company's internal compliance program is a factor that can increase the amount of an award, and that a whistleblower's interference with internal compliance and reporting is a factor that can decrease the amount of an award.

VI. Conclusion

Whether the new whistleblower provisions will have a significant or a negligible impact on FCPA enforcement remains to be seen. In any event, corporations, individuals, and their counsel should be aware of the potential consequences associated with FCPA violations and the provisions of the Dodd-Frank Act's SEC whistleblower program.

APPENDIX A – Pharmaceutical and Medical Device Companies and the FCPA

AstraZeneca PLC

On April 28, 2011, AstraZeneca disclosed that it received inquiries from the DOJ and SEC in connection with an investigation into FCPA issues in the pharmaceutical industry across several countries. "AstraZeneca is cooperating with these inquiries and is investigating, among other things, sales practices, internal controls, certain distributors, and interactions with healthcare providers, institutions, and other government officials. AstraZeneca is investigating inappropriate conduct in certain countries, including China."[29]

Lilly Eli & Co.

"In August 2003, we received notice that the staff of the SEC is conducting an investigation into the compliance by Polish subsidiaries of certain pharmaceutical companies, including Lilly, with the U.S. Foreign Corrupt Practices Act of 1977."[30]

Johnson & Johnson

In February 2007, J&J voluntarily disclosed to the DOJ and the SEC that non-U.S. subsidiaries may have violated the FCPA through improper payments in connection with the sale of medical devices in two small-market countries.[31]

In April 2011, J&J paid $70 million ($21.4 million criminal fine via a DOJ DPA; $48.6 million in disgorgement and prejudgment interest via a SEC settlement) to resolve FCPA enforcement actions for conduct in Greece, Poland, Romania and an investigation of J&J subsidiary companies in the United Nations Oil-for-Food Program in Iraq.[32] J&J also paid approximately $7.9 million in a related U.K. Serious Fraud Office civil recovery action against its company DePuy International Limited, a subsidiary of DePuy Incorporated.[33]

Medtronic, Inc.
On September 25, 2007, the SEC sent Medtronic a letter requesting information relating to potential FCPA violations, such as payments to government-employed doctors, in connection with the sale of medical devices in foreign countries, including Greece, Poland, Germany, Turkey, Italy, and Malaysia.[34]

Merck & Co., Inc.
"The Company has received letters from the DOJ and the SEC that seek information about activities in a number of countries and reference the Foreign Corrupt Practices Act. The Company is cooperating with the agencies in their requests and believes that this inquiry is part of a broader review of pharmaceutical industry practices in foreign countries."[35]

Novo Nordisk A/S
In May 2009, Novo Nordisk pled guilty and paid a $9 million fine for paying $1.4 million to former Iraqi government officials in the UN Oil-for-Food Program for government contracts to provide insulin and other drugs, and Novo also paid $3,025,066 in civil penalties and $6,005,079 in disgorgement of profits.[36]

Syncor Taiwan, Inc.
In December 2002, Syncor pled guilty and paid $2 million in criminal fines and $500,000 in civil penalties.[37]

Zimmer Holdings, Inc.
In September 2007, the SEC informed Zimmer that it was investigating potential FCPA violations in medical device sales in foreign countries by companies, and that in November 2007, the DOJ requested any information provided to the SEC also be provided to the DOJ on a voluntary basis.[38]

1. Author of treatise, Federal False Claims Act and Qui Tam Litigation, Law Journal Press (2010), research source of the issues discussed in this article.
2. *See* 15 U.S.C. § 78dd-2(a) (domestic concerns); 15 U.S.C. § 78dd-1 (issuers).
3. *See* S.Rep. No. 114 at 4, 1977 U.S. Code Cong. & Admin. News at 4101 (testimony of Treasury Secretary W. Michael Blumenthal that in many nations, such payments are illegal). For example, in the United Kingdom, the Serious Fraud Office enforces its overseas corruption laws, and in Canada, the Corruption of Public Officials Act is the equivalent of the FCPA in the United States.

4. *See United States v. Castle*, 925 F.2d 831 (5th Cir. 1991) (per curiam) (holding that foreign officials who take bribes cannot be prosecuted under the FCPA or the general conspiracy statute and discussing the policy decisions behind Congress' decision to exclude foreign officials from prosecution).
5. *See* 15 U.S.C. § 78dd-2(h)(1) (defining "domestic concern").
6. *See* 15 U.S.C. § 78dd-1(a).
7. *See* 15 U.S.C. § 78dd-2(h)(5) (defining "interstate commerce").
8. *See* 15 U.S.C. § 78dd-1(f)(1) (defining "foreign official" but not defining "instrumentality" of a foreign official); 15 U.S.C. § 78dd-2(h)(2) (same).
9. *See United States v. Kozeny*, 493 F. Supp. 2d 693, 704 (S.D.N.Y. 2007) (defining "corruptly" as being beyond the element of "general intent" present in most criminal statutes and defining it as "a bad or wrongful purpose and an intent to influence a foreign official to misuse his official position"), *aff'd*, 541 F.3d 166 (2d Cir. 2008); S. Rep. No. 95-114, at 10 (1977) (According to the Senate Report for the FCPA, "the word 'corruptly' connotes evil motive or purpose, an intent to wrongfully influence the recipient.").
10. *See* Jury Instructions in *United States v. Bourke*, S2 05-cr-518 (SAS) (S.D.N.Y.); *Bryan v. United States*, 524 U.S. 184, 191 (1998) (holding that to prove that a defendant acted "willfully," the government must prove that the defendant knew his conduct was unlawful); *United States v. Kay*, 513 F.3d 432, 448-50 (5th Cir. 2007) (holding that proving a defendant acted "willfully" requires the government to prove that the defendant knew his conduct was unlawful).
11. *See* Jury Instructions in *United States v. Jefferson*, 1:07-CR-209 (E.D. Va. 2009) (For the knowledge element of the FCPA, the court instructed the jury "If the evidence shows you that the defendant actually believed the transaction was legal, he cannot be convicted, nor can he be convicted of being stupid or negligent or mistaken. More is required than that.").
12. 15 U.S.C. § 78dd-2(h)(2)(A); 15 U.S.C. § 78dd-1(f)(1)(A).
13. *See* 15 U.S.C. § 78dd-2(h)(2)(A); 15 U.S.C. § 78dd-1(f)(1)(A).
14. *See United States v. O'Shea*, No. 09-629 (S.D. Tex.); *United States v. Aguilar*, No. 10-1031 (C.D. Cal.); *United States v. Esquenazi*, No. 09-21010 (S.D. Fla.); *United States v. Carson*, No. 09-00077 (C.D. Cal.).
15. *See* 15 U.S.C. § 78dd-1(f)(2) (defining knowing as used in the FCPA); 15 U.S.C. § 78dd-2(h)(3)(A) (same); *See also* Stipulation re: Further Briefing Regarding Jury Instructions, *United States v. Carson*, No. SA CR 09-00077-JVS (C.D. Ca. Sept. 21, 2011) (stipulation between the government and the defense that the answer to the court's question, "Must he [the defendant] know that the individual is in fact a government official?" is "yes").
16. *See* 15 U.S.C. § 78dd-1(b) (setting forth the exception); 15 U.S.C. § 78dd-2(b) (same); 15 U.S.C. § 78dd-1(f)(3) (defining "routine governmental action"); 15 U.S.C. § 78dd-2(h)(4) (same).
17. *See* 15 U.S.C. § 78dd-1(c)(1); 15 U.S.C. § 78dd-2(c)(1).
18. *See* 15 U.S.C. § 78dd-1(c)(2); 15 U.S.C. § 78dd-2(c)(2).
19. *See* Press Release, Dept. of Justice, *Department of Justice Secures More Than $2 Billion in Judgments and Settlements as a Result of Enforcement Actions Led by*

the Criminal Division, Jan. 21, 2011, *available at* http://www.justice.gov/opa/pr/2011/January/11-crm-085.html.

20. Lanny A. Breuer, Assistant Attorney General, DOJ Criminal Division, Address to the 22nd National Forum on the Foreign Corrupt Practices Act (Nov. 17, 2009), *available at* http://www.justice.gov/criminal/pr/speeches-testimony/documents/11-17-09aagbreuer-remarks-fcpa.pdf.
21. *See* Gardiner Harris, U.S. Inquiry of Drug Makers Is Widened, N.Y. TIMES, Aug. 13, 2010, *available at*http://www.nytimes.com/2010/08/14/health/policy/14drug.html?_r=3&ref=todayspaper (discussing the increase in DOJ and SEC investigations of major drug and device makers regarding illegal payments to doctors and health officials in foreign countries).
22. *See* Appendix A attached hereto for a listing of certain drug and device companies and the FCPA issues each has encountered.
23. *See* Mike Koehler, *The Foreign Corrupt Practices Act in the Ultimate Year of Its Decade of Resurgence*, 43 IND. L. REV. 389, 406 (2010) (noting that "no business entity has publicly challenged either enforcement agency in an FCPA case in the last twenty years").
24. *See* 42 U.S.C. § 1320A-7.
25. *See generally* Drury D. Stevenson & Nicholas J. Wagoner, *FCPA Sanctions: Too Big to Debar?*, 80 FORDHAM L. REV. 775 (2011), *available at* [link removed 3/26/2013 – no longer available].
26. *See Bingham's Michael Levy on the Rise of Prosecutorial Common Law*, 25 Corporate Crime Reporter 6, Feb. 7, 2011, *available at* http://www.corporatecrimereporter.com/michaellevy020711.htm (describing "prosecutorial common law").
27. *See* U.S. Const. art. III, § 1; *Marbury v. Madison*, 1 Cranch 137, 177 (1803) ("It is emphatically the province and duty of the judicial department to say what the law is."); *United States v. Nixon*, 418 U.S. 683, 704 (1974) (noting that judicial powers cannot be shared with the Executive Branch).
28. *See* Joel Androphy, Federal False Claims Act and Qui Tam Litigation, Law Journal Press (2010).
29. AstraZeneca PLC, Form 20-F Annual Report for year ending Dec. 31, 2010, at 13, *available at*http://markets.financialcontent.com/stocks/action/getedgarwindow?accesscode=95010311001574.
30. Lilly Eli & Co, Form 10-Q Quarterly Report for period ending Mar. 31, 2011, at 28, *available at*http://files.shareholder.com/downloads/LLY/1242779432x0xS1193125-11-117877/59478/filing.pdf.
31. Johnson & Johnson, Form 10-Q Quarterly Report for period ending July 4, 2010, at 32, *available at*http://www.sec.gov/Archives/edgar/data/200406/000095012310076076/y84968e10vq.htm.
32. *See* Press Release, Dept. of Justice, *Johnson & Johnson Agrees to Pay $21.4 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act and Oil for*

Food Investigations (Apr. 8, 2011), *available at* http://www.justice.gov/opa/pr/2011/April/11-crm-446.html.
33. *See* Press Release, U.K. Serious Fraud Office, DePuy International Limited ordered to pay 4.829 million pounds in Civil Recovery Order (Apr. 8, 2011), *available at* http://www.sfo.gov.uk/press-room/latest-press-releases/press-releases-2011/depuy-international-limited-ordered-to-pay-4829-million-pounds-in-civil-recovery-order.aspx.
34. Medtronic, Inc., Form 10-K Annual Report for year ending Apr. 24, 2009, at 36, *available at*http://www.sec.gov/Archives/edgar/data/64670/000089710109001266/medtronic092639s2_10k.htm.
35. Merck & Co., Inc., Form 10-Q Quarterly Report for period ending June 30, 2010, at 26, *available at*http://www.sec.gov/Archives/edgar/data/310158/000095012310074336/y83714e10vq.htm.
36. *See* Press Release, Dept. of Justice, *Novo Nordisk Agrees to Pay $9 Million Fine in Connection with Payment of $1.4 Million in Kickbacks Through the United Nations Oil-for-food Program* (May 11, 2009), *available at* http://www.justice.gov/opa/pr/2009/May/09-crm-461.html.
37. *See* Press Release, Dept. of Justice, *Syncor Taiwan, Inc. Pleads Guilty to Violating the Foreign Corrupt Practices Act* (Dec. 10, 2002), *available at*http://www.justice.gov/opa/pr/2002/December/02_crm_707.htm.
38. Zimmer Holdings, Inc., Form 10-K Annual Report for year ending Dec. 31, 2009, at 63, *available at*http://www.sec.gov/Archives/edgar/data/1136869/000095012310017177/c55340e10vk.htm.

Notice

This website is designed to provide general information only. This information is not and should not be construed to be formal legal advice. The transmission of the information found on this website also does not result in the formation of a lawyer-client relationship.

- About
- Practice Areas
- Attorneys
- Results
- In the News
- Offices
- Publications & Presentations
- Fees
- Contact Us
- The Qui Tam Blog

Attorney Advertising. Results obtained depend on the facts of each case. Prior results do not guarantee a similar outcome.

Evolving Trends and Ethical Issues Involving FCA/Qui Tam Enforcement of the Medical Device Industry

Joel M. Androphy
Berg & Androphy
3704 Travis
Houston, Texas 77002
Telephone: (713) 529-5622
Facsimile: (713) 529-3785

CHAPTER NO. 9

CHAPTER 9

Pleadings and Disclosures

Chapter Contents

complaint is so "egregiously defective" that it fails to confer jurisdiction on the court, it would not serve as an effective placeholder to which a government complaint can relate back.[54.1]

[3]—Counterclaims

[a]—Generally Allowed

With limited exceptions, defendants are permitted to assert counterclaims in an FCA suit.[55] This is based on the policy that denying a defendant the ability to assert a counterclaim violates due process.[56]

[b]—Exceptions

[i]—Indemnity and Contribution

A defendant has no right to assert a counterclaim for contribution or indemnity in an FCA case.[57] In the event the relator is personally

---

transactions or occurrences set forth, or attempted to be set forth, in the prior complaint . . . ." (emphasis added). See 31 U.S.C. § 3731(c).

[54.1] See United States *ex rel.* Robinson-Hill v. Nurses' Registry and Home Health Corp., 2012 WL 4598699 at *5 (E.D. Ky. Oct. 2, 2012) (citing In re Pharmaceutical Industry Average Wholesale Price Litigation, 498 F. Supp. 2d 389, 399 (D. Mass. 2007).

[55] See United States *ex rel.* Madden v. General Dynamics Corp., 4 F.3d 827, 830-831 (9th Cir. 1993). For example, defamation claims are based on state law. A defendant will generally be permitted to bring a defamation claim because the claim will most likely be compulsory under Federal Rule of Civil Procedure 13. In this event, the relator may assert affirmative defenses of the fair reporting privilege or fair comment. Wells v. Liddy, 186 F.3d 505, 518 n.10 (4th Cir. 1999).

See also, Cell Therapeutics Inc. v. Lash Group Inc., 586 F.3d 1204 (9th Cir. 2009) (concluding that although generally a party found liable under the FCA may not attempt to shift FCA liability to another allegedly liable party, this does not prevent a liable party from bringing independent claims against such a third party).

[56] *Id.* (*United States ex rel. Madden v. General Dynamics Corp.*) 4 F.3d at 831. Denying a defendant the opportunity to assert an independent counterclaim (a claim that does not depend on the defendant's liability, as opposed to an action to offset liability) would be an affront to procedural due process, because Federal Rule of Civil Procedure 13 requires the defendant to bring counterclaims in the suit or risk being unable to raise them later. *Id.* See also, United States *ex rel.* Hartman v. Allegheny General Hospital, 2005 WL 2106627, at *15 (W.D. Pa. Aug. 26, 2005). That case affirmed the rule in *Madden. Id.* The relator argued that counterclaims were not permitted in *qui tam* actions. The court rejected that contention, and cited *Madden* in holding that "[c]ounterclaims that seek damages on claims unrelated to the allegedly fraudulent claims under the False Claims Act are permitted." *Id.*

[57] *Second Circuit:* United States *ex rel.* Mikes v. Straus, 931 F. Supp. 248, 261 (S.D.N.Y. 1996) ("Any attempt by defendants to offset their FCA liability by seeking contribution or indemnification from the relator is futile."); United States *ex rel.* Rodriquez v. Weekly Publications, 74 F. Supp. 763, 769 (S.D.N.Y. 1947) (holding that a defendant could not counterclaim for indemnity because it would discourage relators from bringing FCA suits).

Ninth Circuit: Mortgages, Inc. v. United States District Court for the District of Nevada, 934 F.2d 209, 214 (9th Cir. 1991); United States *ex rel.* Stephens v. Prabhu,

implicated in the FCA violation, the only remedy Congress provided was a reduced share of the recovery.[58] Courts have also not allowed

---

163 F.R.D. 340 (D. Nev. 1995) (dismissing third-party claims that sought indemnity and contribution from third-party defendants for any proven FCA liability); United States v. Kennedy, 431 F. Supp. 877, 878 (C.D. Cal. 1977) (holding that if the defendant was liable for FCA violation, he is not permitted indemnification from a third party even if the third party is jointly and severally liable under the FCA).

In *Mortgages, Inc. v. United States District Court for the District of Nevada, id.*, the Nevada District Court denied the relator's motion to dismiss the defendant's third-party complaints seeking indemnity and contribution. *Id.*, 934 F.2d at 211. The relator then applied for a writ of *mandamus* from the Ninth Circuit. In this case, the defendant had applied for federally insured loans from the relator's mortgage lending company (*id.*, 934 F.2d at 210) and allegedly included false and misleading statements on the loan applications. After the defendant defaulted on the loans, HUD covered several million dollars in losses, and the relator agreed to indemnify the government for $437,000 in a settlement agreement. The relator then filed an FCA suit against the defendants and the government intervened. *Id.*, 934 F.2d at 210-211. The defendant counterclaimed with several state law claims, and sought indemnity and/or contribution from the relator in the event the defendant would have to pay a judgment to the government. *Id.*, 934 F.2d at 211. The district court refused to dismiss the defendant's counterclaims. *Id.*

On the *mandamus* petition, the Ninth Circuit analyzed whether the defendant had the right to contribution or indemnity from the relator. *Id.*, 934 F.2d at 212. In the decision, the court assumed that the relator and the defendant were both responsible for the false statements in the loan applications. Although the defendant asserted state law indemnity and contribution claims, the court considered whether these rights were created federally because if there was no right to indemnity or contribution under federal law, there would be no right in a state law claim. *Id.*, 934 F.2d at 213. Generally, a defendant has the right to contribution or indemnification where the right is expressly or implicitly created by Congress or arises under federal common law. *Id.*, 934 F.2d at 212 (citing Texas Industries, Inc., v. Radcliff Materials, 451 U.S. 638, 101 S.Ct. 2061, 2065, 68 L.Ed.2d 500 (1981)). The *Mortgages, Inc.* court found that the text of the FCA does not include the right to contribution or indemnity, nor is there any indication in the legislative history that it existed. *Id.*, 934 F.2d at 213. Instead, the legislative history indicated that Congress was aware that wrongdoers might be rewarded because the FCA provisions "are based upon the idea of 'setting a rogue to catch a rogue.'" *Id.* (quoting Cong. Globe, 37th Cong., 3d Sess. 955-956 (1863)). In addition, the court found that there is no state right to seek such relief under the federal common law. *Mortgages, Inc. v. United States District Court for the District of Nevada, id.*, 934 F.2d at 214.

The court addressed three possible ways a federal common law right might arise, and found no support within the FCA for any of them. That is, the court has the right to apply federal common law:

> (1) "where a federal rule of decision is necessary to protect uniquely [*sic*] federal interest";
>
> (2) "when a statute contains sweeping language and its legislative history indicates Congress's expectation that the courts will give shape to the statute's broad mandate by drawing on common-law tradition"; and
>
> (3) in an area "dominated by strong national or federal concerns such as controversies between states, admiralty matters, or foreign relations." *Id.*, 934 F.2d at 213. (Internal quotation marks and citations omitted.)

Therefore, there is no right to assert state law claims that would have the same result. *Id.*, 934 F.2d at 214. The writ of *mandamus* was granted. *Id.*

[58] See 31 U.S.C. § 3730(d)(3):

third-party claims for contribution and indemnification, whether there is a *qui tam* relator or the action is initiated by the United States.[59]

[ii]—Counterclaims Against the Government

Sovereign immunity generally prevents a party from asserting a counterclaim against the Government. However, in FCA cases some courts have recognized a limited waiver of this sovereign immunity where the Government has intervened and when "the counterclaims arises out of the same transaction or occurrence as the government claims and the relief neither exceeds nor differs in kind from that sought by the United States."[60]

The Fifth Circuit has distinguished between permissive and compulsory counterclaims in determining whether sovereign immunity is available to protect the state from a defendant's counterclaims.[61] When the state initiates an action, the state waives sovereign immunity only to those counterclaims that are compulsory.[62] Compulsory counterclaims are claims that arise out of the same transaction that is the subject matter of the opposing party's counterclaim.[63] However, if the counterclaim is permissive, i.e., does not meet the same subject

---

"Whether or not the Government proceeds with the action, if the court finds that the action was brought by a person who planned and initiated the violation of section 3729 upon which the action was brought, then the court may, to the extent the court considers appropriate, reduce the share of the proceeds of the action which the person would otherwise receive under paragraph (1) or (2) of this subsection, taking into account the role of that person in advancing the case to litigation and any relevant circumstances pertaining to the violation. If the person bringing the action is convicted of criminal conduct arising from his or her role in the violation of section 3729, that person shall be dismissed from the civil action and shall not receive any share of the proceeds of the action. Such dismissal shall not prejudice the right of the United States to continue the action, represented by the Department of Justice." (Emphasis added.)

See also, United States *ex rel.* Mikes v. Straus, 931 F. Supp. 248, 261 (S.D.N.Y. 1996) (explaining that Section 3730(d)(3) "merely reduces the amount that may be awarded to the relator from the proceeds recovered by the government from the violator. . . .").

[59] Israel Discount Bank, LTD v. Entin, 951 F.2d 311, 315 (11th Cir. 1992) (*dictum*).

[60] United States *ex rel.* Fallon v. Accudyne Corp., 921 F. Supp. 611, 617-618 (W.D. Wis. 1995). In United States v. Q International Courier, Inc., 131 F.3d 770 (8th Cir. 1997), the Government sued Q International, a mail courier firm, for violations of the False Claims Act. *Id.*, 131 F.3d at 772. Q International counterclaimed against the Government, alleging that the United States Post Office violated the Lanham Act by engaging in unfair competition. The court found that the Government did not waive its sovereign immunity under the Lanham Act, but because the U.S. Postal Service had a "sue and be sued" clause (39 U.S.C. § 401(1)), the Government had waived its sovereign immunity. *Id.*, 131 F.3d at 775.

[61] Texas v. Caremark Inc., 584 F.3d 655, 659 (5th Cir. 2009).

[62] *Id.*

[63] *Id.*

matter test, then the state can still assert sovereign immunity, even if the state initiated the lawsuit.[64]

Counterclaims have been allowed against the government pursuant to this waiver of sovereign immunity under the doctrine of recoupment.[65] Courts have not allowed counterclaims for breach of contract, or those based on the Declaratory Judgment Act or the Mandamus Act.[66] In Medicare cases where the defendant seeks set-offs against the Department of Health and Human Services, the counterclaim must comply with Title 42 U.S.C. Section 405(h), which provides for judicial review of claims arising under the Medicare Act only after the Secretary of the Department of Health and Human Services has rendered a final judgment.[67] Defendants who assert counterclaims against the government for recoupment must, however, exhaust all available administrative remedies before bringing the counterclaims; otherwise, the court may dismiss the counterclaims under Rule 12(b)(6).[68]

[iii]—Counterclaims Arising Out of Relator's Employment

A relator will generally be protected while he is collecting evidence of an FCA violation.[69] Common claims against an employee for gathering an employer's documents include breach of confidentiality agreement, breach of fiduciary duty, and conversion.[70] Although a duty

---

[64] *Id.*

[65] United States v. Agnew, 423 F.2d 513, 514 (9th Cir. 1970). If the defendant is a government contractor, the recoupment counterclaim will be governed by the Contract Disputes Act ("CPA"), Pub. L. No. 95-563, 92 Stat. 2383 (Nov. 1, 1978), as amended; 41 U.S.C. § 605(a). The Federal Tort Claims Act ("FTCA"), Pub. L. No. 79-601, Title IV, 60 Stat. 812 (Aug. 2, 1946), significantly amended by Pub. L. No. 89-506, 80 Stat. 306 (July 18, 1966), and thereafter—especially 28 U.S.C. § 2680(a)—is another possible basis for a counterclaim against the government; however, there is not much case law on whether this theory will ultimately be successful.

[66] Declaratory Judgment Act, Pub. L. No. 80-773, 62 Stat. 964 (June 25, 1948), as amended; 28 U.S.C. § 2201, Fed. R. Civ. P. 57. Mandamus Act, Pub. L. No. 87-748, § 1(a), 76 Stat. 744 (Oct. 5, 1962), 28 U.S.C. § 1361. Thomas v. Pierce, 662 F. Supp. 519, 524 (D. Kan. 1987).

[67] See:

Third Circuit: United States *ex rel.* Kirsch v. Armfield, 56 F. Supp.2d 588, 592-593 (W.D. Pa. 1998).

Sixth Circuit: United States v. Royal Geropsychiatric Services, 8 F. Supp.2d 690. 696-697 (N.D. Ohio 1998).

[68] United States v. Kellogg Brown & Root Services, Inc., 2012 WL 1382986, at *1, *5 (D.D.C. April 23, 2012) (the court lacked jurisdiction over the recoupment counterclaim because the defendant failed to exhaust the available administrative remedies).

[69] See United States *ex rel.* Yesudian v. Howard University, 153 F.3d 731, 740 (D.C. Cir. 1998).

[70] See United States *ex rel.* Grandeau v. Cancer Treatment Centers of America, 350 F. Supp.2d 765, 772-774 (N.D. Ill. 2004). See also, United States ex rel. Santa

of loyalty to the employer generally does exist, strong public policy supports protecting the employee who believes in good faith that the employer is engaged in unlawful activity.[71] However, several district courts have allowed for some recovery on a breach of contract counterclaim.[72] For example, in *United States ex rel. Cafasso v. General Dynamics C4 Systems, Inc.*, the district court allowed the recovery of attorney's fees on a breach of contract counterclaim against an employee who took documents from her employer in direct violation of her employment contract.[73] The relator argued that she was privileged to take the documents for discovery purposes in order to prove her *qui tam* claim against the defendant.[74] The court, however, found that in removing the documents, she was not cooperating in a government investigation, reporting fraud, or preserving evidence.[75] Rather, the court found that the relator obtained the documents without regard to whether the documents pertained to the specific claims she intended to bring and that the relator had no reason to believe that the defendant company was going to alter, destroy, or falsify the documents in question.[76] The court, however, reduced the amount of the award based on the extreme hardship to the relator.[77]

Ana v. Winter Park Urology Associates, P.A., 2012 WL 2886617 (M.D. Fl. July 13, 2012) (denying a counterclaim for breach of fiduciary duty without prejudice and granting leave to allow defendant to amend).

[71] See:

Eighth Circuit: Kempcke v. Monsanto Co., 132 F.3d 442, 445 (8th Cir. 1998) (holding that "[a]n employee with a good faith reason to believe his employer is engaged in unlawful age discrimination 'has a legitimate interest in preserving evidence of [his employer's] unlawful employment practices'") (quoting O'Day v. McDonnell Douglass Helicopter Co., 79 F.3d 756, 763 (9th Cir. 1996)).

Ninth Circuit: United States *ex rel.* Cafasso v. General Dynamics C4 Systems, Inc., 2009 WL 3723087, at *10 (D. Ariz. Nov. 4, 2009) (the court held that the relators might have a good reason not to tell employers of their intent to sue under the FCA and that such belief does not indicate that a relator brought the claim in bad faith).

District of Columbia Circuit: United States *ex rel.* Head v. Kane Co., 668 F. Supp.2d 146, 154 (D.D.C. 2009) (holding that the employment agreement did not require the relator to turn over correspondence and records he gathered from the defendant because to require the return of this evidence would unduly frustrate the purpose of the FCA).

[72] See United States *ex rel.* Cafasso v. General Dynamics C4 Systems, Inc., 2009 WL 3723087 (D. Ariz. Nov. 4, 2009), *aff'd* 637 F.3d 1047 (9th Cir. 2011); Glynn v. Impact Science & Technology, Inc., 2011 WL 3792358 (D. Md. Aug. 25, 2011).

[73] *United States ex rel. Cafasso v. General Dynamics C4 Systems, Inc.*, *id.*, 2009 WL 3723087, at *5.

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.*

According to the Department of Justice, a relator cannot be held civilly liable for conduct that the FCA encourages and protects.[78] The Department of Justice further contends that

> "in order for [a] relator to proceed with an FCA action, the FCA requires that relators disclose to the United States alone 'substantially all material evidence and information the person possesses,' 31 U.S.C. § 3730(b)(2), and ties relator's share to the importance of her participation in the action and the relevance of the information she provided. . . . Not only does the FCA contemplate that relators will share evidence with the government, but also that they will do so in secrecy."[79]

The Department of Justice further states that the purpose of the seal provisions is to "protect the Government's interest in criminal matters" and to enable the government to investigate the alleged violations without tipping off the defendant at a "sensitive stage."[80] The only unresolved area is whether a relator may rummage through proprietary and corporate files that he would not have access to in the normal scope of his employment. Most attorneys would caution their clients not to engage in this potentially improper search.[81]

(Text continued on p. 9-31)

---

[78] Submission of the United States as *Amicus Curiae* in Support of Relator's Motion to Dismiss Counterclaims, United States *ex rel.* Grandeau v. Cancer Treatment Centers of America, No. 99 C8287, at 5 (N.D. Ill. April 6, 2004).

[79] Submission of the United States as *Amicus Curiae* in Support of Relator's Motion to Dismiss Counterclaims, United States *ex rel.* Grandeau v. Cancer Treatment Centers of America, No. 99 C8287, at 7 (April 6, 2004) (citing United States *ex rel.* Green v. Northrop Corp., 59 F.3d 953, 964 (9th Cir. 1995)).

See generally, Grimm, "Courageous Whistleblowers Are Not 'Left Out in the Cold': Legitimate Justifications Exist for Collecting Evidence of False Claims Act Violations," 39 TAF Q. Rev. 127 (Oct. 2005).

[80] *Id.* (Submission of the United States) at 8 (citing United States *ex rel.* Yesudian v. Howard University, 153 F.3d 731, 743 (D.C. Cir. 1998)).

[81] See generally, Herzfeld, "Gathering Evidence in Qui Tam Cases Raises Ethical Tensions, Speakers Say," Health Care Fraud Rep. (BNA) 1019 (Dec. 15, 2010) (discussing in detail the gathering of evidence by employees for *qui* tam filings and its ethical ramifications).

Furthermore, it is reasonable to obtain copies of employer documents, rather than originals, to prove fraud.[82] Retaining mere copies of documents does not rise to the level of deprivation of the employer's property that is required to constitute conversion.[83] Moreover, at least one court has held that in addition to using the documents to prove fraud, a former employee is not required to return the documents to his employer.[84]

Relators have expressed concern that their employers could use the Computer Fraud and Abuse Act ("CFAA") against them.[85] The CFAA prohibits employees from "knowingly access[ing] a computer without authorization or exceeding authorized access" to obtain information for improper purposes.[86] Although the law was intended to prevent employees from stealing data to compete with their employer,[87] employee rights attorneys worry that employers may use the CFAA against employees who are exposing company fraud and other wrongdoing.[88] In addition, the CFAA does not require proving that the defendant actually removed or copied information from a computer in order to establish a violation.[89]

Recently, courts have allowed prosecutors to bring charges under the CFAA against defendants for violating their employer's computer use policies and access restrictions.[90] In *United States v. Teague*, the Eighth

---

[82] See X Corp. v. Doe, 805 F. Supp. 1298, 1311-1312 (E.D. Va. 1992), *aff'd* 17 F.3d 1435 (4th Cir. 1994).

[83] See: Pearson v. Dodd, 410 F.2d 701, 706 (D.C. Cir. 1969); Furash & Co., Inc. v. McClave, 130 F. Supp.2d 48, 58 (D.D.C. 2001).

[84] *X Corp. v. Doe*, N. 82 *supra*, 805 F. Supp. at 1311-1312.

[85] Baldas, "Crackdown on Taking Company Trade Secrets: Extreme Competition, Fluid Work Force Bring More Employer Actions," The Nat'l L.J. 4 (Oct. 1, 2007). And see The Computer Fraud and Abuse Act ("CFFA"), Pub. L. No. 99-474, § 2, 100 Stat. 1213 (Oct. 16, 1986), as amended.

[86] 18 U.S.C. § 1030.

[87] Ackerman, "Suing Employees for Computer Fraud Gets Easier," The Nat'l L.J. 36, (Oct. 31, 2011).

[88] Baldas, N. 85 *supra*, at 4.

[89] S. Rep. No. 99-432, 99th Cong., 2d Sess. at 4 (Sept. 3, 1986), reprinted in 1986 U.S. Code Cong. & Admin. News 2479, 2483.

[90] See:

Third Circuit: United States v. Tolliver, 451 Fed. Appx. 97, 103-104 (3d Cir. 2011) (a defendant violated Section 1030 by exceeding her authorized access when she "intentionally accessed the customer's accounts" without a "business purpose" for so doing).

Fifth Circuit: United States v. John, 597 F.3d 263, 269, 273 (5th Cir. 2010) ("[W]hen an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access' within the meaning of § 1030(a)(2).").

Circuit upheld a conviction where the defendant merely looked at computer records that she was not authorized to access.[91] United States v. Teague, 646 F.3d 1119, 1123 (8th Cir. 2011). See also Ackerman, N. 87 *supra*, at 36. The First Circuit, however, declined to extend CFAA liability to a defendant who accessed documents without authorization merely to "satisf[y] idle curiosity."[92] The Ninth Circuit has limited the scope of the CFAA to "the unauthorized procurement or alteration of information, not its misuse or misappropriation."[93]

[4]—Preliminary Injunctions

A court may grant a preliminary injunction in an FCA case as part of its equitable powers.[94] To determine whether the Government is entitled to an injunction, the court will consider three issues: (1) Does the party in favor of the injunction "seek cognizable relief in equity involving assets of the defendant"; (2) is the preliminary injunction "a reasonable measure to preserve the *status quo* in aid of the ultimate equitable relief claimed"; and (3) is the public interest at stake, mandating heightened interest of the court?[95]

The Ninth Circuit has distinguished between independent claims and dependent claims in determining whether a counterclaim is a

---

Seventh Circuit: International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (a terminated employee no longer had authorization to access company computers and thus could not "access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"). (Internal quotation marks omitted.)

Eleventh Circuit: United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (*en banc*), *cert. denied* ___ U.S. ___, 131 S.Ct. 2166 (2011) ("[The defendant's] use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access. Rodriguez exceeded his authorized access and violated the Act when he obtained personal information for a nonbusiness reason.").

[91] United States v. Teague, 646 F.3d 1119, 1123 (8th Cir. 2011). See also Ackerman, N. 87 supra, at 36.

[92] United States v. Teague, 646 F.3d 1119, 1123 (8th Cir. 2011). See also Ackerman, N. 87 *supra*, at 36.

[93] United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).

[94] United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (quoting Shamrock Foods Co. v. Gast, 535 F. Supp.2d 962, 965 (D. Ariz. 2008)).

[95] See:

Fourth Circuit: United States *ex rel.* Rahman v. Oncology Associates, P.C., 198 F.3d 489, 502 (4th Cir. 1999); United States *ex rel.* Taxpayers Against Fraud v. The Singer Co., 889 F.2d 1327, 1335 (4th Cir. 1989) (affirming district court's granting of preliminary injunction against defendants in FCA case).

Seventh Circuit: United States *ex rel.* Flewelling v. DBB, Inc., 180 F.3d 1277, 1286 (7th Cir. 1999) (allowing a preliminary injunction under 18 U.S.C. Section 1345(a)(2)(B) in an FCA case).

Ch. 9 Rel. 19 Update

Insert A:

Defendants are generally permitted to assert counterclaims in FCA suits, however, there are two exceptions where counterclaims may not be asserted: where a counterclaim would violate public policy and where a counterclaim is dependent on the *qui tam* defendant's liability.[1] These restrictions on counterclaims are permissible because they do not completely deny the defendant's ability to assert counterclaims, which would violate due process. [keep FN 56].

Insert B:

Courts have held that a defendant may not pursue counterclaims that are equivalent to contribution or indemnification.[2]

---

[1] **keep original text in FN 55 and add:** United States v. Campbell, No. 08-1951, 2011 WL 43013, at *10 (D.N.J. Jan. 4, 2011).

[2] *Fifth Circuit*: U.S. ex rel. Longhi v. United States, 575 F.3d 458, 474 (5th Cir. 2009). ("To enforce the release and indemnification clauses contained in the stock sale agreement against [relator] would ignore the public policy objectives expressly spelled out by Congress in the FCA and would provide disincentives to future relators.")
Seventh Circuit: U.S. v. Omnicare, Inc., No. 07 C 05777, 2013 WL 3819671 (N.D. Ill. June 23, 2013) (dismissing counterclaims where they would essentially be a contribution or indemnification); U.S. ex rel. Wildhirt v. AARS Forever, Inc., No. 09 C 1215, 2013 WL 5304092 (N.D. Ill. Sept. 19, 2013) (counterclaims that are equivalent of contribution or indemnification are prohibited under the FCA).
Ninth Circuit: Mortgages, Inc. v. United States District Court for the District of Nevada, 934 F.2d 209, 213 (9th Cir. 1991) ("The FCA is in no way intended to ameliorate the liability of wrongdoer by providing defendants with a remedy against a qui tam plaintiff with 'unclean hands.' Congress did not intend to create a right of action for contribution or indemnification under the FCA.").
Eleventh Circuit: Israel Disc. Bank Ltd. v. Entin, 951 F.2d 311, 313 (11th Cir. 1992) (Affirming district court's holding that "under no circumstances was an indemnity or contribution claim authorized under the FCA.").

Insert C:

In *Mortgages, Inc. v. United States District Court for the District of Nevada*, the Nevada District Court denied the relator's motion to dismiss the defendant's third-party complaints seeking indemnity and contribution.[3] On mandamus petition, the Ninth Circuit considered whether the right to contribution and indemnity was created by federal law.[4] If no such federal right existed, then there would be no right in the state law claims for this type of relief.[5] Generally, a defendant has the right to contribution or indemnification where the right is expressly or implicitly created by Congress or arises under federal common law.[6] The Ninth Circuit held that the text of the FCA does not include the right to contribution or indemnity, nor is there any indication in the legislative history that it existed.[7] Instead, the legislative history indicated that Congress was aware that wrongdoers might be rewarded because the FCA provisions "are based upon the idea of setting a rogue to catch a rogue."[8] In addition, the court held that there is no state right to seek such relief under the federal common law.[9] Therefore, there is no right to assert state law claims that would have the same result.[10]

Insert D:

[iii] Counterclaims for Independent Damages

In contrast to claims for indemnification and contribution, claims for independent damages are permitted under the FCA.[11] "Independent damage"

---

[3] Id. at 211.
[4] Id.
[5] Id. at 213.
[6] Id., 934 F.2d at 212 (citing Texas Industries, Inc., v. Radcliff Materials, 451 U.S. 638, 101 S.Ct. 2061, 2065, 68 L.Ed.2d 500 (1981)).
[7] Id., 934 F.2d at 213.
[8] Id. (quoting Cong. Globe, 37th Cong., 3d Sess. 955-956 (1863)).
[9] Mortgages, Inc. v. United States District Court for the District of Nevada, 934 F.2d at 214.

> The court addressed three possible ways a federal common law right might arise, and found no support within the FCA for any of them. That is, the court has the right to apply federal common law:
>
> > (1) where a federal rule of decision is necessary to protect uniquely [sic] federal interest;
> > (2) when a statute contains sweeping language and its legislative history indicates Congress's expectation that the courts will give shape to the statute's broad mandate by drawing on common-law tradition; and
> > (3) in an area dominated by strong national or federal concerns such as controversies between states, admiralty matters, or foreign relations.
>
> Id., 934 F.2d at 213. (Internal quotation marks and citations omitted.)

[10] Id. at 934.
[11] U.S. ex rel. Madden v. Gen. Dynamics Corp., 4 F.3d 827, 830-31 (9th Cir. 1993).

counterclaims are claims in which the outcome does not depend on whether the defendant is found liable as to the underlying FCA claim.[12]

In *U.S. ex rel. Madden v. General Dynamics Corporation*, the defendant asserted several counterclaims directed at the *qui tam* relators: breach of duty of loyalty and fiduciary duty, breach of implied covenant of good faith and fair dealing, violations of the state labor code, libel, fraud, interference with economic relations, and misappropriation of trade secrets.[13] In reversing the district court's dismissal of the defendant's counterclaims, the Ninth Circuit distinguished counterclaims seeking indemnity and contribution from counterclaims seeking independent damages, holding that the former are barred under the FCA but the latter must be permitted.[14] The court held that as to counterclaims for independent damages, the defendant's due process rights outweigh the government's interest in encouraging relators to bring suit, noting that these types of counterclaims are often compulsory, requiring the defendant to assert them in the relator's suit or risk being unable to raise them at a later time.[15]

The court clarified that allowing claims for independent damages to proceed is consistent with the principle of disallowing indemnity and contribution counterclaims: "if a *qui tam* defendant is found liable, the counterclaims [for independent damages] can then be dismissed on the ground that they will have the effect of providing for indemnification or contribution. On the other hand, if a qui tam defendant is found not liable, the counterclaims can be addressed on the merits."[16]

In deciding whether a defendant's counterclaims against the relator employee should be permitted, several courts have made a distinction between dependent and independent claims.[17] For example, in *U.S. ex rel. Battiata v. Puchalski*, the relators brought a *qui tam* action against their former employer for obtaining improper payments by

---

[12] Id. at 830-31 ("Counterclaims for indemnification or contribution by definition only have the effect of offsetting liability. Counterclaims for independent damages are distinguishable, however, because they are not dependant on a qui tam defendant's liability.").
[13] U.S. ex rel. Madden v. Gen. Dynamics Corp., 4 F.3d 827, 829.

[14] Id. at 831.
[15] Id.
[16] Id.
[17] U.S. ex rel. Head v. Kane Co., 668 F. Supp. 2d 146, 153 (D.D.C. 2009); U.S. ex rel. Miller v. Bill Harbert Int'l Const., Inc., 505 F. Supp. 2d 20, 26 (D.D.C. 2007); Cell Therapeutics, Inc. v. Lash Grp., Inc., 586 F.3d 1204, 1208 (9th Cir. 2009), as amended on denial of reh'g and reh'g en banc (Jan. 6, 2010); Walsh v. Amerisource Bergen Corp., No. CIV.A. 11-7584, 2014 WL 2738215, at *4 (E.D. Pa. June 17, 2014)

submitting bills using incorrect service codes.[18] The defendant then asserted several counterclaims against the relators for malicious prosecution, tortious interference with economic relations, abuse of process, breach of fiduciary duty, indemnification and contribution, unjust enrichment, and mistake of fact.[19] In analyzing the viability of the counterclaims, the court examined whether the counterclaims were dependent or independent of the employer's liability in the *qui tam* suit.[20]

Using this analysis, the court dismissed with prejudice the defendant's claims for breach of fiduciary duty, indemnification and contribution, unjust enrichment, and mistake of fact, holding that these claims were *dependent* on the outcome of the FCA suit.[21] The court found that the remaining counterclaims arguably sought *independent* damages.[22] Nevertheless, the court dismissed the defendant's remaining counterclaims without prejudice due to insufficient pleadings, but it did not foreclose the defendant's ability to replead them.[23] This holding is consistent with other district court decisions, such as *Ruhe* and *Head*, in which the court dismissed counterclaims made by employers against employees rooted in contract provisions created to preclude *qui tam* litigation, such as confidentiality and non-disclosure agreements.[24]

In *Town of Newton v. Rumery*, the Supreme Court held that a private agreement is unenforceable if enforcement is clearly outweighed by a public policy against such terms.[25] Although a duty of loyalty to the employer generally does exist, strong public policy supports the protection of employees who believe in good faith that the employer is engaged in unlawful activity.[26] Thus, typically a counterclaim that a relator breached a duty of loyalty is not supportable.

In *Wildhirt v. AARS Forever, Incorporated*, an Illinois District Court agreed with the rationale in *Cafasso*, holding that *qui tam* relators who

---

[18] U.S. ex rel. Battiata v. Puchalski, 906 F. Supp. 2d 451, 453 (D.S.C. 2012).
[19] Id.
[20] Id.
[21] Id. at 461.
[22] Id.
[23] Id. at 462
[24] See e.g., U.S. ex rel. Ruhe v. Masimo Corp., 929 F. Supp. 2d 1033, 1038 (C.D. Cal. 2012); U.S. ex rel. Head v. Kane Co., 668 F. Supp. 2d 146, 149 (D.D.C. 2009).
[25] Town of Newton v. Rumery, 480 U.S. 386, 107 S.Ct. 1187, 94 L.Ed.2d 405 (1987).
[26] Keep FN 71 the same.

retain or disclose confidential information going beyond the scope necessary to pursue their suit may not avoid a defendant's counterclaims for breach of contract.[27] In *Wildhirt*, the employee relators signed agreements stating that they knew of no "suspect" practices, they would report any such practices to the employer before pursuing a *qui tam* suit, and they would indemnify the employer for any attorneys' fees incurred in a *qui tam* suit where confidential employer information was improperly disclosed.[28] Subsequently, the relators filed suit without first alerting the employer to the practices that they claimed were unlawful.[29] The employees also took home confidential documents, without knowledge of any fraudulent practices, and made harmful statements about the employer to the Veteran's Administration before pursuing their *qui tam* suit.[30] The court acknowledged that dependent counterclaims having an equivalent effect of contribution and indemnity are not allowed.[31] However, the court held that the counterclaims were independent due to the extremely broad scope of the documents retained, therefore, the court held, the counterclaims' success would not require as an essential element that Defendants be held liable under the FCA.[32]

Insert E:

Common claims against an employee for gathering an employer's documents include: breach of contract, breach of fiduciary duty, indemnification and contribution, unjust enrichment, mistake of fact, malicious prosecution, tortious interference with economic relations, abuse of process, and conversion.[33] In allowing or disallowing counterclaims stemming from the employment relationship, courts generally seek to

---

[27] U.S. ex rel. Wildhirt v. AARS Forever, Inc., No. 09 C 1215, 2013 WL 5304092, at *6 (N.D. Ill. Sept. 19, 2013).
[28] Id. at 2.
[29] Id. at 5.
[30] Id.
[31] Id.
[32] Id. at 6.; See also, United States v. Cancer Treatment Centers of Am., No. 99 C 8287, 2005 WL 300414, at *2 (N.D. Ill. Feb. 4, 2005) (concealing a subpoena addressed to the company is not protected); U.S. ex rel. Hartman v. Allegheny Gen. Hosp., No. CIV.A. 02-1948, 2005 WL 2106627, at *5 (W.D. Pa. Aug. 26, 2005) (deleting, destroying, or altering company documents were considered independent claims).
[33] U.S. ex rel. Battiata v. Puchalski, 906 F. Supp. 2d 451, 453 (D.S.C. 2012).

balance the employer's interest in protecting confidential information and the government's interest in encouraging employees to disclose fraud.[34]

Insert F:

; Siebert v. Gene Sec. Network, Inc, No. 11-CV-01987-JST, 2013 WL 5645309, at *8 (N.D. Cal. Oct. 16, 2013) (declining to dismiss counterclaim for breach of confidentiality agreement when it was possible that relator took documents that bore no relation to his FCA claim).

But See United States v. Cancer Treatment Centers of Am., 350 F. Supp. 2d 765, 773 (N.D. Ill. 2004) (Relator could not be held liable for breach of confidentiality agreement because such an agreement "cannot trump the FCA's strong policy of protecting whistleblowers who report fraud against the government.... Relator could have disclosed the documents to the government under any circumstances, without breaching the confidentiality agreement.")

---

[34] See United States v. Northrop Corp., 59 F.3d 953, 964 (9th Cir. 1995) ("In carefully crafting provisions that specify the relator's recovery and in amending the jurisdictional provisions, it is clear that Congress attempted to walk a fine line between encouraging whistle-blowing and discouraging opportunistic behavior."); United States v. Cancer Treatment Centers of Am., 350 F. Supp. 2d 765, 773 (N.D. Ill. 2004) ("[T]he confidentiality agreement cannot trump the FCA's strong policy of protecting whistleblowers who report fraud against the government.").

Evolving Trends and Ethical Issues Involving FCA/Qui Tam Enforcement of the Medical Device Industry

Joel M. Androphy
Berg & Androphy
3704 Travis
Houston, Texas 77002
Telephone: (713) 529-5622
Facsimile: (713) 529-3785

CHAPTER NO. 9A

CHAPTER 9A

Pretrial Motions and Discovery

Chapter Contents

[5]—Sanctions

If a party fails to comply with discovery, the opposing party can file a motion to compel disclosure or to compel a discovery response.[34] If the court grants the motion to compel, the moving party can recover its reasonable associated costs, including attorney's fees.[35] In addition, if a party fails to comply with a court's discovery order, the court may impose various sanctions including:

(1) making an adverse inference against the non-complying party;
(2) barring the non-complying party from asserting certain claims or defenses;
(3) "striking pleadings in whole or in part";
(4) staying the proceedings until the party complies with the discovery order;
(5) "dismissing the action in whole or in part";
(6) "rendering a default judgment against the disobedient party"; or
(7) holding the disobedient party in contempt of court.[36]

The court can also impose costs in addition to or instead of the sanctions listed above.[37]

The Fourth Circuit has adopted a four-part test for spoliation sanctions that requires the court to determine:

"(1) whether the noncomplying party acted in bad faith,(2) the amount of prejudice that noncompliance caused the adversary, (3) the need for deterrence of the particular sort of noncompliance, and (4) whether less drastic sanctions would have been effective."[38]

In *United States v. Universal Health Services, Inc.*, the court denied a motion to impose an adverse inference when the defendant did not change its policy of recording over old surveillance videos even after the court issued a discovery order because the defendant had not acted in bad faith.[39] In addition, in order to find that spoliation

---

[34] Fed. R. Civ. P. 37(a).
[35] Fed. R. Civ. P. 37(a)(5)(A).
[36] Fed. R. Civ. P. 37(b)(2)(A)(i) to 37(b)(2)(A)(vii).
[37] Fed. R. Civ. P. 37(b)(2)(B).
[38] United States v. Universal Health Services, Inc., 2011 WL 2559552, at *4 (W.D. Va. June 28, 2011) (quoting Anderson v. Foundation for Advancement, Education and Employment of American Indians, 155 F.3d 500, 504 (4th Cir. 1998)).
[39] *Id.*, 2011 WL 2559552, at *1-*4. The adverse spoliation inference allows the jury to assume that evidence destroyed by a party would likely have been adverse to

occurred so that a sanction may be imposed, "a court must first find that the evidence previously existed."[40]

Courts also possess inherent authority to impose sanctions against parties that violate discovery orders and rules.[41] Under its inherent authority, a court can impose sanctions when a party had notice or knowledge "that evidence in dispute was 'potentially relevant' to probable litigation and [the opposing party] was prejudiced by [the litigant's] conduct."[42] When a party deliberately destroys or alters evidence in a way "that undermine[s] the integrity of the judicial proceedings," a court can use its inherent authority to dismiss the case because the offending party "has willfully deceived the court and engaged in conduct utterly inconsistent with the orderly administration of justice."[43] For example, in *United States ex rel. Berglund v. Boeing Co.*, the court imposed monetary sanctions against the relator and dismissed one of the complaints after the relator altered emails and destroyed hard drives in order to bolster his claims against the defendant.[44]

Federal courts have become more consistent in their rules and rulings on e-discovery and spoliation issues.[45] District courts tend not to impose severe sanctions for minor infractions, allowing for consistent results throughout the circuits.[46] In addition to the promulgation by courts of clearer rules, judges, attorneys, and parties have become more knowledgeable about e-discovery requirements, reducing the number of sanctions imposed.[47] Moreover, some circuits have adopted pilot programs to reduce discovery disputes through increased cooperation between the parties.[48]

---

its interests. *Id.*, 2011 WL 2559552, at *3. For this sanction to apply, the disobedient party must have acted more than negligently. *Id.*

[40] *Id.*, 2011 WL 2559552, at *5.

[41] United States *ex rel.* Berglund v. Boeing Co., 2011 WL 6182109, at *27 (D. Ore. Dec. 13, 2011). Under its inherent authority, a court can impose sanctions that include: "(1) excluding spoiled evidence; (2) admitting evidence of the circumstances of the destruction or spoliation; or (3) instructing the jury that it may infer that the spoiled or destroyed evidence would have been unfavorable to the responsible party." *Id.*, 2011 WL 6182109, at *30 (citing Glover v. BIC Corp., 6 F.3d 1318, 1329 (9th Cir. 1993)).

[42] *Id.*, 2011 WL 6182109, at *28.

[43] *Id.*, 2011 WL 6182109, at *31 (quoting Leon v. PIX Sys. Corp,, 464 F.3d 951, 958 (9th Cir. 2006)).

[44] *Id.*, 2011 WL 6182109, at *22-*26.

[45] Tadler and Kelston, "Fears of Discovery Burden Are Exaggerated," The Nat'l L. J. 18 (Dec. 19, 2011).

[46] *Id.*

[47] *Id.*

[48] *Id.*