Patient Privacy in the US

Brian Taylor, Esq.
btaylor@boutinjones.com

Boutin Jones INC
ATTORNEYS AT LAW

Privacy in the US Overview

- Children's Online Privacy Protection Act (COPPA) – 15 U.S. C. § 6501
- Family Educational Rights and Privacy Act of 1974 (FERPA) – 20 U.S.C. § 1232g
- Fair Credit Reporting Act (FCRA) – 15 U.S.C. §§ 1681-1681u
- Driver's Privacy Protection Act of 1994 – 18 U.S.C. § 2721
- Fair Debt Collection Practices Act – 15 U.S. C. §§ 1692-1692p
- Federal Privacy Act of 1974 – 5 U.S.C. § 552a
- Financial Services Modernization Act of 1999, Privacy Rule – 15 U.S.C. §§ 6801-6809
- Video Privacy Protection Act of 1988 – 18 U.S.C. § 2710
- Computer Fraud and Abuse Act of 1984 – 18 U.S.C. § 1030
- Computer Matching & Privacy Protection Act of 1988 & Amendments of 1990 – 5 U.S. Code § 552a (a)(8)-(13), (e)(12), (o), (p), (q), (r), & (u)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Patient Privacy–General Guidelines

All generalizations are false, including this one.

–Mark Twain

Boutin Jones INC
ATTORNEYS AT LAW

Patient Privacy in the US Overview

- HIPAA: Health Insurance Portability and Accountability Act of 1996.
  - Goal: to save money for health care businesses by encouraging electronic transactions and also to protect the security and confidentiality of patient information.

BoutinJones INC
ATTORNEYS AT LAW

HIPAA—To Whom Does It Apply?

- **"Covered Entities"**
  - Health plans;
  - Healthcare clearinghouses;
  - Health care providers who transmit health information in electronic form.
- **Business Associates**
  - A person or organization, other than a covered entity, that performs certain functions for a covered entity that involve the use or disclosure of individually identifiable health information—legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

HIPAA—What Information is Protected?

- **Protected Health Information "PHI" is:**
  - "Individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **PHI includes:**
  - An individual's physical or mental health condition,
  - The provision of health care to the individual, or
  - The payment for the provision of health care; and
  - That identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
- **Common identifiers such as name, address, birth date, social security number.**

BoutinJones INC
ATTORNEYS AT LAW

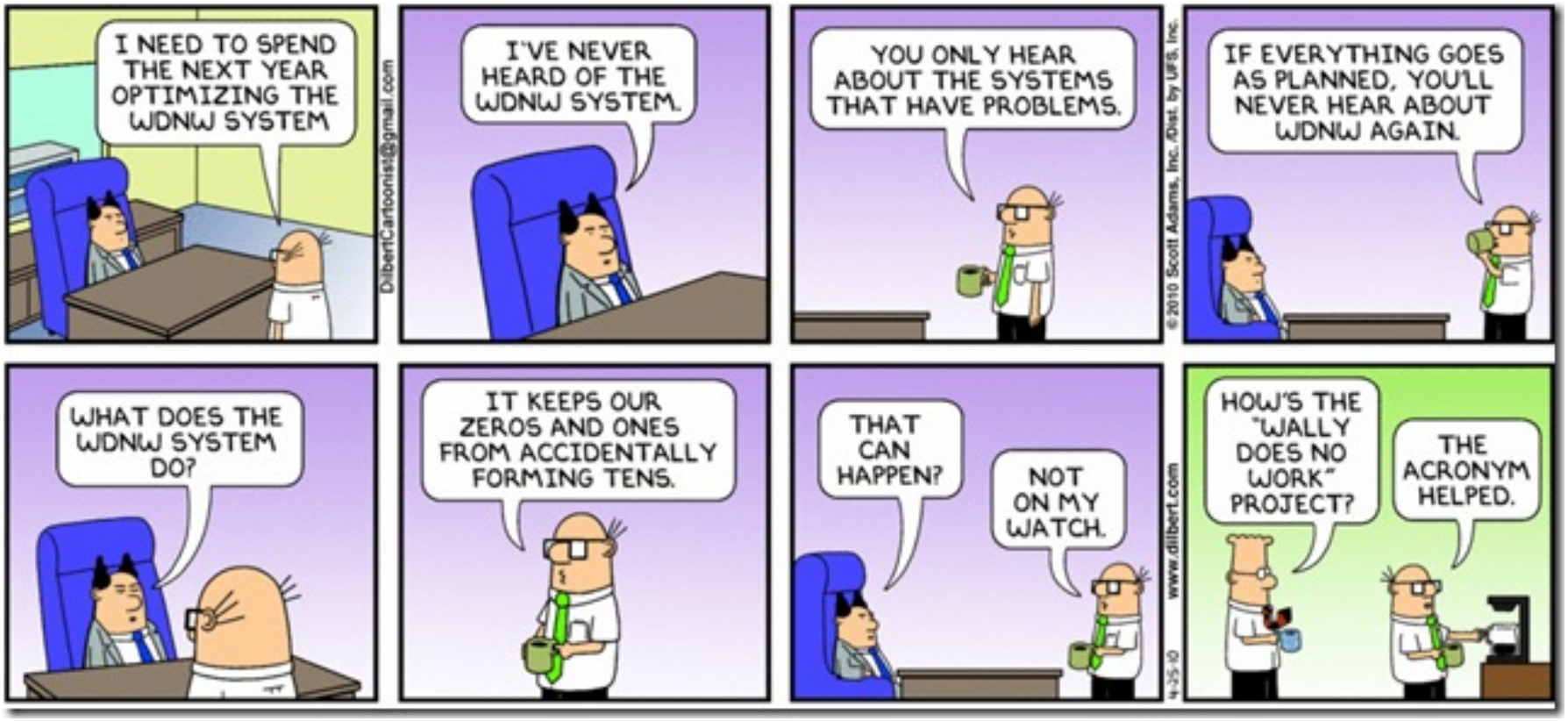
HIPAA—When Can PHI Be Disclosed?

- Under the HIPAA Privacy Rule, PHI may be used or disclosed by a covered entity without first obtaining a member authorization for:
  1. Treatment;
  2. Payment;
  3. Health care operations;
  4. Public Policies Reasons—controlling disease, injury , or disability; FDA regulated products; communicable diseases; work related illness or injury; victims of abuse; health oversight; judicial and administrative proceeding or subpoena; law enforcement activities; research; etc.
- Authorizations are required to use PHI for other purposes (e.g., marketing).

HIPAA—HITECH

- Final regulations implementing the "Health Information Technology for Economic and Clinical Health (HITECH) Act," enacted as part of the "American Recovery and Reinvestment Act of 2009" (ARRA). In general, the new rules:
  1. Expand the obligations of physicians and other health care providers to protect PHI;
  2. Extend security obligations to business associates; and
  3. Increase the penalties for violations of any of these obligations.

HIPAA "HITECH"



BoutinJones INC
ATTORNEYS AT LAW

HIPAA—Enforcement and Penalties

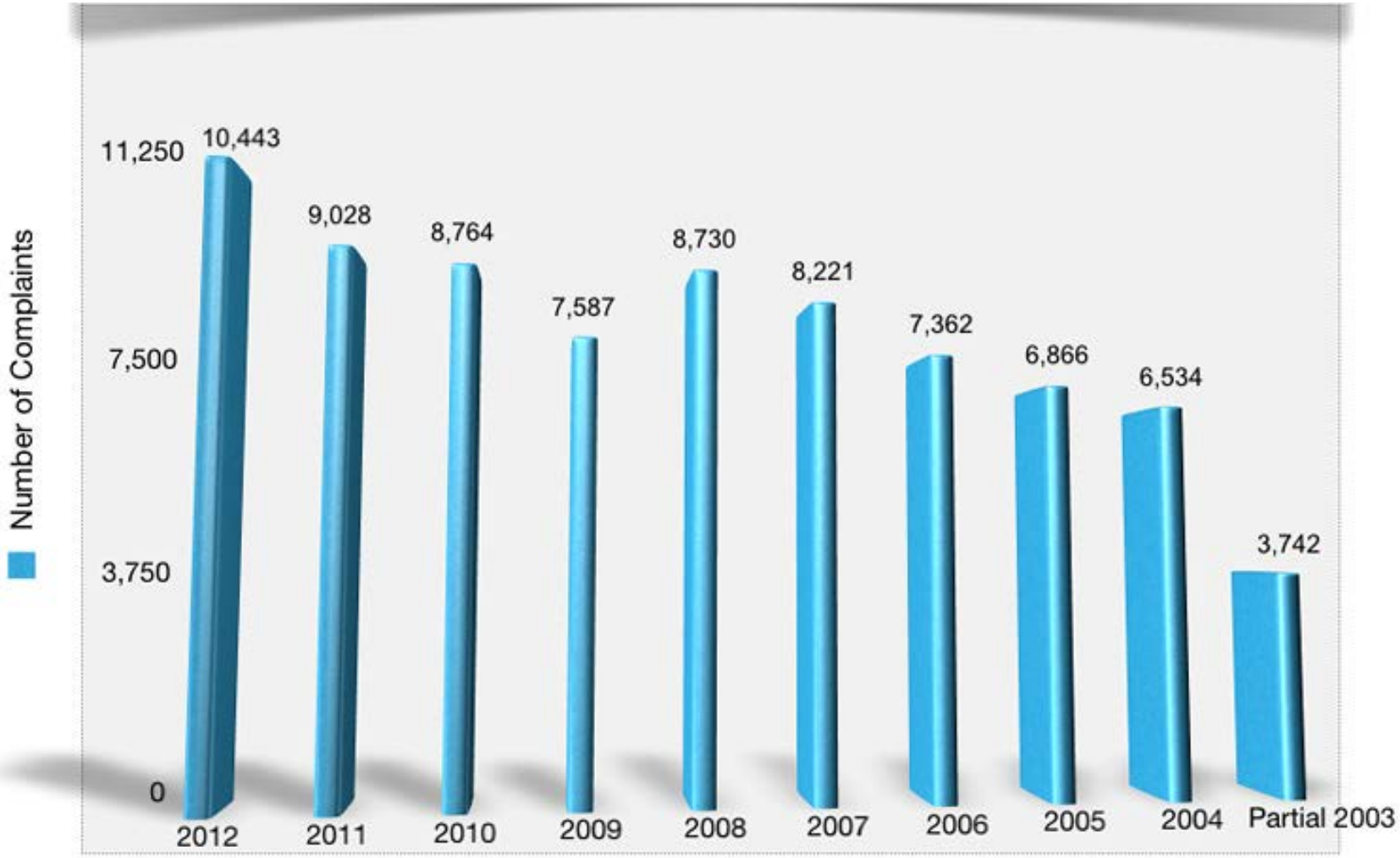
- Enforced by Department of Health and Human Services, Office for Civil Rights ("OCR")
- Penalties vary significantly depending on factors such as the date of the violation, whether the covered entity know or should have knows of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect.

	Prior to 2/18/09	After 2/18/09
Penalty Amount	Up to $100 per violation	$100 to $50,000 or more per violation
Calendar Year Cap	$25,000	$1,500,000

HIPAA—Enforcement and Penalties; cont'd

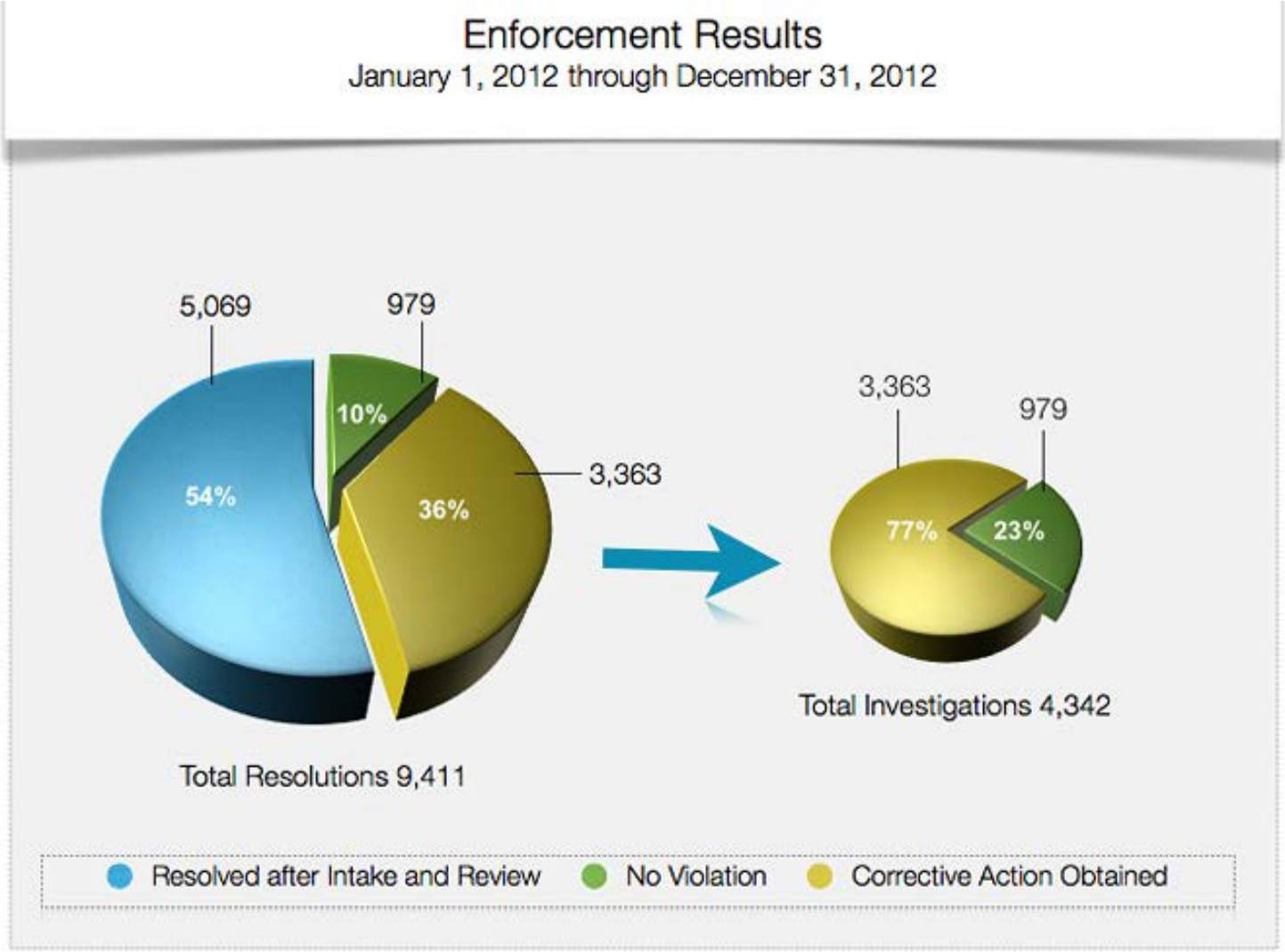
- Criminal penalties: A person who knowingly obtains or discloses PHI in violation of HIPAA may face a criminal penalty or up to $50,000 and up to one-year imprisonment. The criminal penalties increase to $100,000 and up to five years imprisonment if wrongful conduct involves false pretenses, and to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm.

HIPAA—Complaints to HHS



BoutinJones INC
ATTORNEYS AT LAW

HIPAA—Complaints to HHS



BoutinJones INC
ATTORNEYS AT LAW

HIPAA—Breach & Enforcement Examples

- Affinity Health Plan, Inc. settled HIPAA violations for $1,215,780. Affinity was informed by a representative of CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity. CBS informed Affinity that the copier that Affinity had used contained confidential medical information on the hard drive. Affinity estimated that up to 344,579 individuals may have been affected by this breach.

HIPAA—Breach & Enforcement Examples

- Shasta Regional Medical Center (SRMC) agreed to a comprehensive corrective action plan and to pay $275,000 to an HHS concerning violations of HIPAA Privacy Rule. A patient was part of news article wherein she asserted that SRMC diagnosed her with and treated her for a condition that she did not have in order to increase SRMC's reimbursement from Medicare. Officers of SRMC later met with a reporter and shared portions of patients medical record to rebut patient's assertions. SRMC asserted the disclosure was appropriate because the patient had "waived" privacy. HHS disagreed: "When senior level executives intentionally and repeatedly violate HIPAA by disclosing identifiable patient information, OCR will respond quickly and decisively to stop such behavior," said OCR Director Leon Rodriguez. "Senior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients' rights are fully protected." The State of California fined Shasta Regional $95,000.

HIPAA—Preemption

- **State laws that are contrary to the HIPAA are preempted:**
  - "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of HIPAA.
- **Exceptions to Preemption for State Laws that:**
  1. Relate to privacy of PHI and provide greater protections to privacy;
  2. Provide for the reporting of disease or injury, child abuse, birth, or death;
  3. Certain health plan reporting, such as for management or financial status.

Privacy in California . . . Wow.

- Automobile "Black Boxes"
- Bank Account Numbers, Reuse
- Computer Misuse and Abuse
- Consumer Credit Reporting Agencies Act
- Court Records: Protection of Victim and Witness
- Credit Card Address Change
- Credit Card/Telephone Service Address Change
- Credit Card or Check Payment
- Credit Card Full Disclosure Act
- Credit/Debit Card Number Truncation
- Credit Card "Skimmers"
- Credit Cards, Substitutes
- Disposal of Customer Records
- Domestic Violence Victim Privacy
- Driver's License Information Confidentiality
- Eavesdropping or Skimming RFID (radio frequency identification)
- Electronic Eavesdropping
- Electronic Eavesdropping by State Law Enforcement Officials
- Electronic Surveillance in Rental Cars
- Employment of Offenders
- Fair Debt Collection Practices Act
- Financial Information Privacy Act
- Information Practices Act of 1977 -
- Information-Sharing Disclosure, "Shine the Light"
- Insurance Information and Privacy Protection Act
- Investigative Consumer Reporting Agencies Act
- Library Records
- Locking Mail Boxes in Residential Hotels
- Marketing to State University Alumni
- Marriage Licenses
- Marriage Records
- Motor Vehicle Dealer Data Access
- Office of Privacy Protection
- Physical & Constructive Invasions of Privacy
- Public Records Act
- Public Record Exemption for Sex Offense Victims
- Reader Privacy Act
- Research
- Security Breach
- Security of Personal Information
- Social Security Number
- Social Security Number Confidentiality in Family Court Records
- Social Security Number Truncation on Pay Stubs
- Social Security Numbers in Abstracts of Judgments, Decrees, and Tax
- Social Security Numbers in Local Government Records
- Supermarket Club Card Act
- Telecommunications Customer Privacy
- Telephone Record "Pretexting"
- Veterans' Discharge Papers, Notice of Public Record Status
- Voter Privacy
- Workplace Surveillance

Health Privacy in California

- **Health Facilities Data Breach – California Health & Safety Code section 1280.15.** This law requires certain health facilities to prevent unlawful or unauthorized access to, or use or disclosure of, a patient's medical information.
- **Medical Information Confidentiality – California Civil Code sections 56-56.37.** This law puts limits on the disclosure of patients' medical information. It specifically prohibits many types of marketing uses and disclosures. It requires an electronic health or medical record system to protect the integrity of electronic medical information and to automatically record and preserve any change or deletion.

Health Privacy in California--Penalties

- Compensatory Damages
- Punitive damages not to exceed $3,000
- Nominal damages of $1,000 (does not require actual or the threat of actual damages)
- Attorneys fees not to exceed $1,000
- Any violation that results in economic loss or personal injury to a patient is punishable as a misdemeanor
- Administrative fine or civil penalty not to exceed $2,500 per violation
- Any person, other than a licensed health care profession, who knowingly and willfully obtains, discloses, or uses medical information in violation shall be liable for administrative fine or civil penalty not to exceed $25,000 per violation

Health Privacy in California--Penalties

- Health care professional who knowingly and willfully obtains, discloses, or uses medical information in violation shall be liable for administrative fine or civil penalty not to exceed $2,500 for first violation, $10,000 second violation, $25,000 third and subsequent violation
- Any person who knowingly and willfully obtains, discloses, or uses medical information for the purpose of financial gain in violation shall be liable for administrative fine or civil penalty not to exceed $250,000 per violation

Questions?

Obedience of the law is demanded; not asked as a favor.

–Theodore Roosevelt

Brian Taylor, Esq.
btaylor@boutinjones.com