

BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

What Keeps Directors and Officers Up at Night

*Critical Issues Facing Corporations, Their Board
Members and Officers*

April 11, 2012

BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

CHARTIS 



EXPAND YOUR EXPECTATIONSSM

Today's Presenters

Baker Donelson

- John Calender – jcalender@bakerdonelson.com
- Tonya Grindon – tgrindon@bakerdonelson.com
- Scott Sherman – ssherman@bakerdonelson.com
- Gary Shockley – gshockley@bakerdonelson.com
- Matt Sweeney – msweeney@bakerdonelson.com
- Steve Wood – sfwood@bakerdonelson.com

Chartis

- David McMahan david.mcmahan@chartisinsurance.com.

KPMG

- Scott Hilsen shilsen@kpmg.com

The Life of a Securities Case

Scott Sherman – Shareholder

Baker Donelson/Atlanta

Matt Sweeney – Shareholder

Baker Donelson/Nashville

David McMahan – AVP/ Regional Manager

Chartis/Atlanta

Scott Hilsen – Director

KPMG/Atlanta

The Life of a Securities Case

What situations can cause shareholder class actions?

- ✓ Stock drop
- ✓ Internal investigation resulting in required disclosure to the public
- ✓ Announcement of merger or acquisition or after the fact disclosure related to the same

The Life of a Securities Class Action

- Filing of the lawsuit
- Possibility of multiple actions
 - Same claims
 - Same jurisdiction
 - Different jurisdiction
 - Related claims (breach of fiduciary duty, shareholder derivative action)
 - Same jurisdiction
 - Different jurisdiction



The Life of a Securities Class Action, cont'd.

- Dispositive Motions
 - Stricter pleading standards
 - Related cases
- Discovery – its cost and timing
 - Pre-suit strategies
 - Stays
- Settlements
 - Money
 - Coupons
 - Disclosures
 - Attorney's Fees



Effects of Securities Class Actions

- Practical implications – 10-Q, 10-K or 8-K disclosures
- Internal investigations
- Derivative lawsuits
- Government investigations (SEC or DOJ)

M&A Litigation



- Injunction frequently sought
- Expedited and expensive
- Whatever the sale price, expect a lawsuit
- Settlements

Private Company Securities Lawsuits

- Shareholder and/or membership disputes
 - Class actions rare
 - Breach of fiduciary duty and derivative cases more common
 - Statutory and common law duties
 - Organizational documents

SEC WHISTLEBLOWER BOUNTY PROGRAM

Tonya Mitchem Grindon – Baker Donelson/Nashville

**Chair – Securities and Corporate
Governance Group; Shareholder**

David McMahan – AVP/Regional Manager

Chartis/Atlanta

Scott Hilsen – Director

KPMG/Atlanta



HOW DID WE GET HERE?



Sarbanes-Oxley Act

With the enactment of the Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002):

- Companies with a class of listed securities have been required to develop and implement whistleblower complaint policies and procedures covering accounting and auditing practices.
- Securities Exchange Act § 10A, 15 U.S.C. § 78j-1

The **Dodd–Frank Wall Street Reform and Consumer Protection Act** was signed into law on July 21, 2010.

Section 922 of the Dodd-Frank Act provides incentives to whistleblowers by:

- Awarding to whistleblowers who provide original information leading to a successful Commission enforcement action resulting in monetary sanctions of more than \$1 million between 10% and 30% of the amount recovered in that action.

-
- Final rules were effective August 12, 2011



Provisions of Final Rules

- The Commission is providing incentives for whistleblowers to exhaust internal procedures first.
- The Commission expressed concern that the potential monetary incentives provided to whistleblowers may reduce the effectiveness of a company's existing compliance, legal audit and similar internal processes for investigating and responding to potential violations of federal securities laws.

Provisions of Final Rules, cont'd

- To balance these competing issues, the rules provide, in effect, that when a whistleblower internally reports a complaint, he will be deemed to have submitted his complaint to the Commission and will not lose the characterization as the “original source” of the information so long as the whistleblower submits his claim to the Commission within 90 days.

Provisions of Final Rules, cont'd

- The Commission stated in its release that in order to encourage whistleblowers to utilize internal reporting processes, it will give favorable consideration in calculating the amount of an award whether the whistleblower used established internal procedures for the receipt and consideration of complaints and misconduct.

Investor Protection and Transparency

- When determining where in the 10-30% realm the award should fall, the SEC must take into account various factors, such as the significance of the information and the degree of the assistance provided.

Investor Protection and Transparency, cont'd

- The Act also establishes the Investor Protection Fund, which is to be funded by collections of certain monetary sanctions, to be the source of the whistleblower payments.

Investor Protection and Transparency, cont'd

- The Act further affords whistleblowers protection (i.e. providing a private cause of action) by preventing employers from discharging, harassing, demoting or taking certain other actions against whistleblowers because of a whistleblower's reporting information to the SEC or providing further assistance to the SEC in an enforcement action.

Investor Protection and Transparency, cont'd

- The action may be brought in federal court and remedies include reinstatement, double back pay with interest and litigation costs.

Key Issues

In response to the new whistleblower program, some companies have taken such actions as:

- Reinforcing their compliance program so that there are more vigorous investigations.
- Enhancing the “net” for internal reporting to allow employees better access.
- Reviewing the code of conduct for anti-retaliation provisions.

Key Issues, cont'd

Investigating allegations can be complicated and time-consuming, and the new rules may be particularly challenging for a company that does not have a well-developed and well-organized program in place.



BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC



Data has Left the Building

Compliance and Risk Management Considerations When
Your Sensitive Information is Out of Your Control

Steve Wood – Baker Donelson/Nashville
Co-Chairman, Emerging Companies Practice
Firm Information Security Officer; Shareholder
David McMahan – AVP/Regional Manager
Chartis/Atlanta
Scott Hilsen – Director
KPMG/Atlanta

EXPAND YOUR EXPECTATIONSSM

“Sensitive Information” is a Broad Category

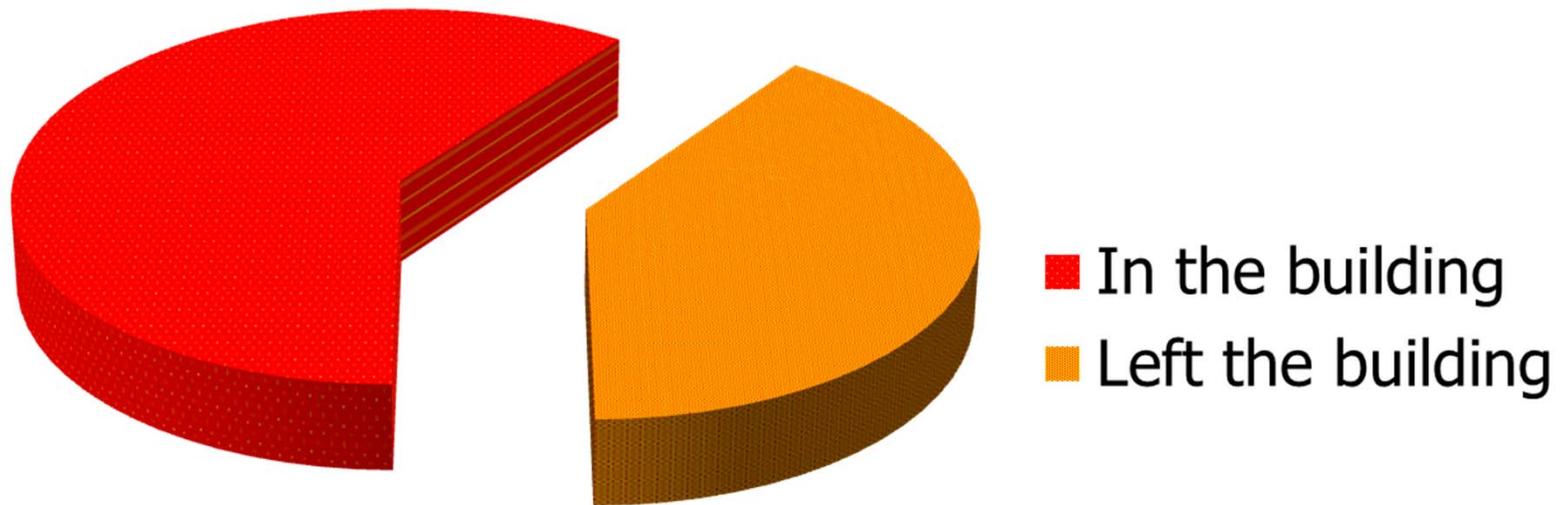
- Patient information
- Customer financial information
- Accounting and financial reporting information
- Credit card information
- Employee health information (for group health plans)
- Employment files
- Company trade secrets
- Trade secrets of customers and strategic partners under NDAs

“Information Security” Defined

Information security management seeks to ensure that sensitive information is:

- ✓ not disclosed except as authorized;
- ✓ not used except as authorized;
- ✓ not modified except as authorized; and
- ✓ available when needed.

The Part of Your Destiny Not in Your Control



Sensitive Information

Where Your Information Lives Away from Home



Employees Removing Information from the Office

- Authorized business purpose
- Inadvertence (or worse)



Third Parties Holding Information under Contract

- Service providers
- Business partners

Where Your Information Lives Away from Home

Employees Removing Information from the Office

- Employees' personal cloud storage accounts (e.g., DropBox)
- Laptops at home or sitting around in airports, hotels, bars, and unoccupied cars
- iPhones and iPads wherever employees (*or directors*) left them
- Forgotten thumb drives in sock drawers
- All of the above for former employees who didn't return them

Third Parties Holding Information under Contract

- Cloud storage vendors
- Software-as-a-service (SaaS) vendors
- Data centers (hosting vendors, etc.)
- Off-site data backup vendors
- Physical files stored offsite
- Decommissioned equipment
- Copiers returned after lease expired
- Strategic and JV partners
- Potential partners/investors/acquirers in due diligence

Regulatory Regimes Implicated

- Sarbanes-Oxley (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standards (PCI-DSS)
- 47 different state data breach laws
- Other state-specific laws on protection and use of personal info

Risks and Potential Liability

- Data breach – unauthorized disclosure or use of information
 - If you can't account for the information and assure that its confidentiality has been maintained at all times, it's a data breach
 - "Risk of harm" threshold *might* apply
 - Breach notification and remediation costs can be very expensive
 - Potential liability to affected individuals and to contract parties for which you hold or manage the data
 - **A data breach downstream in the chain of custody is your breach**
- Regulatory non-compliance (even absent data breach)
 - Civil monetary penalties and fines
 - Costs of government investigations and enforcement actions
 - Potential criminal prosecution for directors and officers

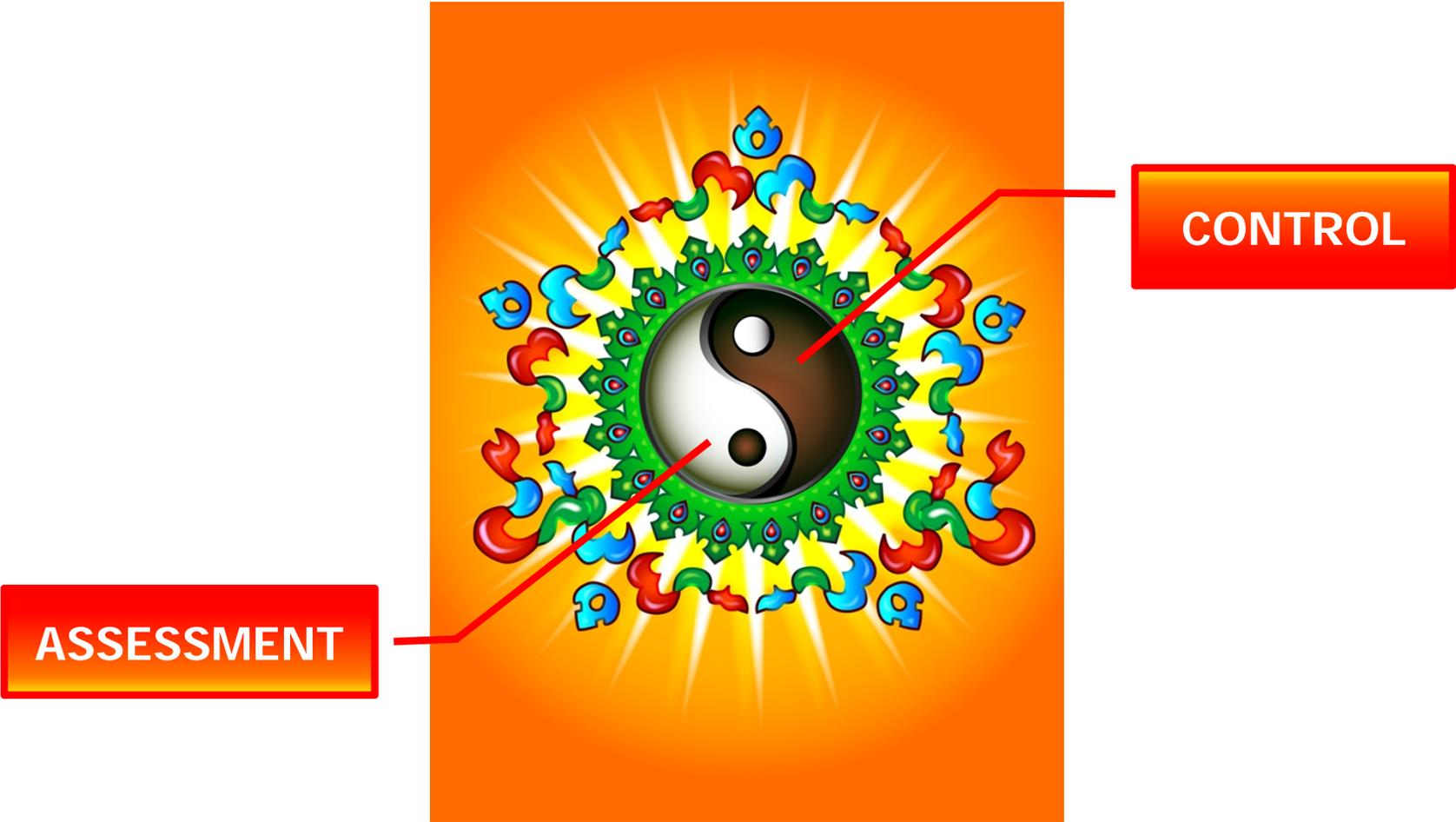
More Reasons to Care About Information Security

- A data breach is likely to be a public relations fiasco
- A data breach may strain relationships even with unaffected customers and strategic partners
- Potential customers and partners increasingly are performing information security due diligence before entrusting companies with their sensitive information or that of their customers
- Poor security and compliance gaps can kill a potential financing or M&A deal
- Having a strong security posture can be a competitive advantage in procuring customers and solidifying business relationship
- How would you want someone to treat your private information???

Security Risk Management and Compliance

How should your company approach the issue?

Security Risk Management 101



Risk Assessment

- Security risk assessment process:
 - 1) Perform information asset inventory (where does your data live?)
 - 2) Determine reasonably plausible vulnerabilities for each asset
 - 3) Evaluate and assign weighting for *likelihood* of each vulnerability
 - 4) Evaluate and assign weighting for *impact* of each vulnerability
 - 5) Multiply weightings for each vulnerability to create risk score
- Objective is to focus attention and resources (i.e., control) on the vulnerabilities having the greatest risk scores
- Remember that information security is a journey, not a destination; it's a process of continuous re-assessment and improvement

Risk Control

- Once identified and appropriately assessed, there are three options for addressing any given risk:
 - **Mitigate it** – implement policies and procedures to reduce likelihood and/or impact of vulnerability
 - **Transfer it** – put the risk off to an insurer or contract party
 - **Accept it** – if unlikely and of limited impact, or if cost to mitigate or transfer is too high
- Note that you cannot control a risk you have not identified

Internal Risk Mitigation Strategies

- Administrative controls
 - Effective, appropriate policies and procedures are the foundation
 - Limit data access and mobility to minimum necessary
 - Security awareness program (training and reminders) is key
 - Regularly perform security risk assessments
- Physical controls
 - Locks, ID badges, etc.
 - Critically important, but not much help as to employees removing information assets to which they have authorized access
- Technical controls
 - Passwords (especially as to mobile devices)
 - Access logs
 - Encryption, encryption, encryption

Risk Mitigation Strategies for Contract Parties

- Due diligence
 - Use preliminary questionnaire
 - Examine policies and procedures
- Covenants
 - Require compliance with applicable regulatory regimes
 - Require formal security management program
 - Consider requiring certification (e.g., ISO 27001)
- Monitoring/reporting
 - Require prompt incident reports and data breach notification
 - Use periodic compliance questionnaires
 - Consider requiring attestation reports (e.g., SOC 2, Type 2)
 - Get inspection/audit rights

Risk Transference Strategies for Contract Parties

- Indemnification for data breach costs
 - Forensics
 - Notification
 - Call center
 - Credit monitoring
 - Legal fees
 - PR efforts
- Ideally, indemnification should be absolute, not conditioned on breach of contract or negligence (or you need to insure the part of the risk not transferred to the contract party)
- Carve-out indemnification from limitation of liability
- Require cyber-liability insurance

Global Anti-Corruption Enforcement: Risky Business – The Whole World's Watching

John Calender – Shareholder

Baker Donelson/Washington, DC

David McMahan – AVP/Regional Manager

Chartis/Atlanta

Scott Hilsen – Director

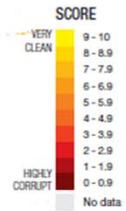
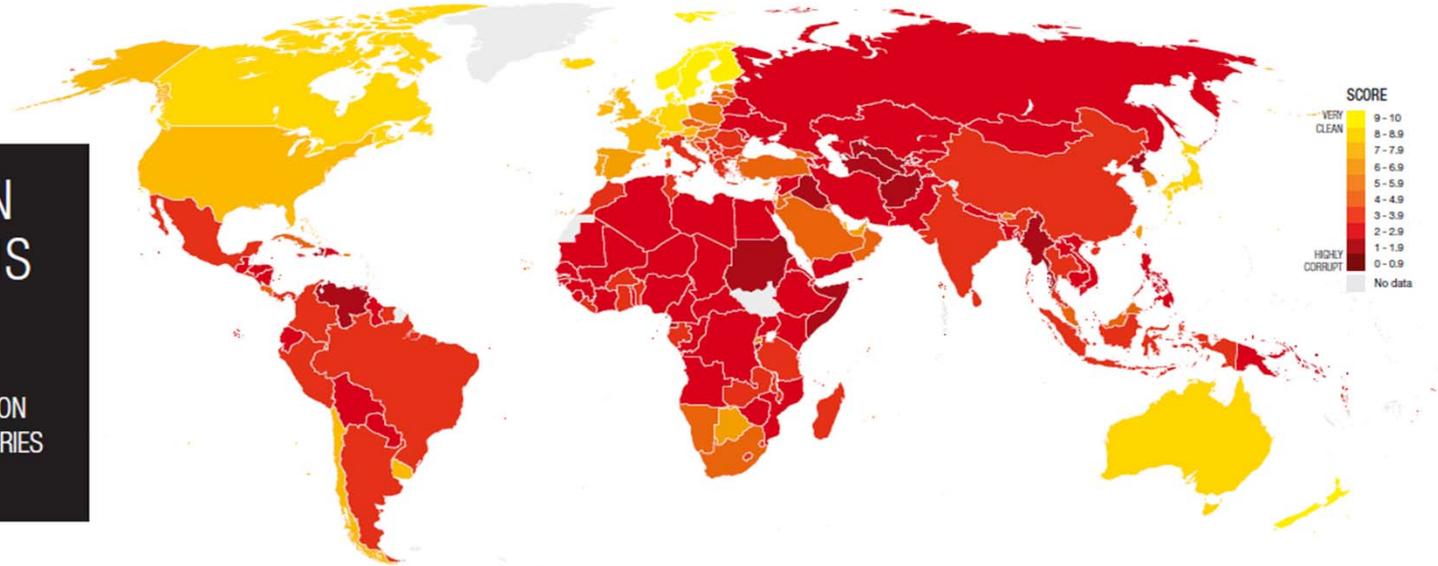
KPMG/Atlanta

Agenda

- Brief Summary of FCPA
- New Developments U.S. and Worldwide on Anti-Corruption
- High Risk Issues
- Best Practices

Transparency International (TI) 2011 World Map

(The TI index is internationally recognized as a barometer of perceived corruption)



CORRUPTION PERCEPTIONS INDEX 2011
THE PERCEIVED LEVELS OF PUBLIC-SECTOR CORRUPTION IN 183 COUNTRIES/TERRITORIES AROUND THE WORLD

RANK	COUNTRY/TERRITORY	SCORE
1	New Zealand	9.5
2	Denmark	9.4
3	Finland	9.4
4	Sweden	9.3
5	Singapore	9.2
6	Norway	9.0
7	Netherlands	8.9
8	Australia	8.8
9	Switzerland	8.8
10	Canada	8.7
11	Luxembourg	8.5
12	Hong Kong	8.4
13	Iceland	8.3
14	Germany	8.0
14	Japan	8.0
16	Austria	7.8
16	Barbados	7.8
16	United Kingdom	7.8
19	Belgium	7.5
19	Ireland	7.5
21	Bahamas	7.3
22	Chile	7.2
22	Qatar	7.2
24	United States	7.1

RANK	COUNTRY/TERRITORY	SCORE
25	France	7.0
25	Saint Lucia	7.0
25	Uruguay	7.0
28	United Arab Emirates	6.8
29	Estonia	6.4
30	Cyprus	6.3
31	Spain	6.2
32	Botswana	6.1
32	Portugal	6.1
33	Taiwan	6.1
35	Slovenia	5.9
36	Israel	5.8
36	Saint Vincent and the Grenadines	5.8
38	Bhutan	5.7
39	Malta	5.6
39	Puerto Rico	5.6
41	Cape Verde	5.5
41	Poland	5.5
43	Korea (South)	5.4
44	Brunei	5.2
44	Dominica	5.2
48	Bahrain	5.1
48	Macao	5.1

RANK	COUNTRY/TERRITORY	SCORE
48	Mauritius	5.1
48	Rwanda	5.0
50	Costa Rica	4.8
50	Lithuania	4.8
50	Oman	4.8
50	Seychelles	4.8
54	Hungary	4.6
54	Kuwait	4.6
55	Jordan	4.5
57	Czech Republic	4.4
57	Namibia	4.4
57	Saudi Arabia	4.4
60	Malaysia	4.3
61	Cuba	4.2
61	Latvia	4.2
61	Turkey	4.2
64	Georgia	4.1
64	South Africa	4.1
66	Croatia	4.0
66	Montenegro	4.0
66	Slovakia	4.0
68	Ghana	3.9
68	Italy	3.9
69	FYR Macedonia	3.9

RANK	COUNTRY/TERRITORY	SCORE
69	Samoa	3.9
73	Brazil	3.8
73	Tunisia	3.8
75	China	3.6
75	Romania	3.6
77	Gambia	3.5
77	Lesotho	3.5
77	Vanuatu	3.5
80	Colombia	3.4
80	El Salvador	3.4
80	Greece	3.4
80	Morocco	3.4
80	Peru	3.4
80	Thailand	3.4
88	Bulgaria	3.3
88	Jamaica	3.3
88	Panama	3.3
88	Serbia	3.3
88	Sri Lanka	3.3
88	Bosnia and Herzegovina	3.2
88	Liberia	3.2
91	Trinidad and Tobago	3.2
91	Zambia	3.2

RANK	COUNTRY/TERRITORY	SCORE
95	India	3.1
95	Kiribati	3.1
95	Swaziland	3.1
95	Tonga	3.1
100	Argentina	3.0
100	Benin	3.0
100	Burkina Faso	3.0
100	Djibouti	3.0
100	Gabon	3.0
100	Indonesia	3.0
100	Madagascar	3.0
100	Malawi	3.0
100	Mexico	3.0
100	Sao Tome and Principe	3.0
100	Tanzania	3.0
100	Turkmenistan	3.0
112	Algeria	2.9
112	Egypt	2.9
112	Kosovo	2.9
112	Moldova	2.9
112	Senegal	2.9
112	Vietnam	2.9
118	Bolivia	2.8
118	Mali	2.8
120	Bangladesh	2.7
120	Ecuador	2.7
120	Ethiopia	2.7
120	Guatemala	2.7
120	Iran	2.7
120	Kazakhstan	2.7
120	Mongolia	2.7
120	Mozambique	2.7
120	Solomon Islands	2.7
128	Armenia	2.6
128	Dominican Republic	2.6
128	Honduras	2.6
128	Philippines	2.6
128	Syria	2.6
134	Cameroon	2.5
134	Entree	2.5
134	Guyana	2.5
134	Lebanon	2.5
134	Maldives	2.5
134	Nicaragua	2.5
134	Niger	2.5
134	Pakistan	2.5
134	Sierra Leone	2.5
143	Azerbaijan	2.4
143	Bolarus	2.4
143	Comoros	2.4
143	Mauritania	2.4
143	Nigeria	2.4
143	Russia	2.4
143	Timor-Leste	2.4
143	Togo	2.4
143	Uganda	2.4
152	Tajikistan	2.3
152	Ukraine	2.3
154	Central African Republic	2.2
154	Congo Republic	2.2
154	Côte d'Ivoire	2.2
154	Guinea-Bissau	2.2
154	Kenya	2.2
154	Laos	2.2
154	Nepal	2.2
154	Papua New Guinea	2.2
154	Paraguay	2.2
154	Zimbabwe	2.2
164	Cambodia	2.1
164	Guinea	2.1
164	Kyrgyzstan	2.1
164	Yemen	2.1

RANK	COUNTRY/TERRITORY	SCORE
168	Angola	2.0
168	Chad	2.0
168	Democratic Republic of the Congo	2.0
168	Libya	2.0
172	Burundi	1.9
172	Equatorial Guinea	1.9
172	Venezuela	1.9
176	Haiti	1.8
176	Iraq	1.8
177	Sudan	1.6
177	Turkmenistan	1.6
177	Uzbekistan	1.6
180	Algeria	1.5
180	Myanmar	1.5
182	Korea (North)	1.0
182	Somalia	1.0

Why Focus on Anti-Corruption?

The consequences of breaching anti-bribery and anti-corruption laws can be far reaching:

FOR INDIVIDUAL:

- Prison Term
- Substantial Fine
- Dismissal
- Loss of reputation
- **THE FINE CANNOT BE PAID DIRECTLY OR INDIRECTLY BY THE COMPANY**
- Substantial Legal Fees
 - Not Reimbursed

FOR COMPANY:

- Substantial Criminal and Civil Fines
- **Disgorgement of Profits**
- Private Damage Actions (Unfair Competition)
- Substantial Legal and Investigative Expenses
- Business Disruption
- Loss of Reputation and Business/Competitive Disadvantage
- Debarment from contracting with Government Customers

Anti-Corruption Fundamentals

FCPA – Prohibits Bribes and Requires Strict Recordkeeping/Accounting Controls

- **Illegal Bribe:** A payment or offer or promise of anything of value, direct or indirect, to foreign official or anyone acting on an official's behalf to affect any governmental act or decision, obtain or retain business or gain improper advantage.
 - Gifts
 - Entertainment, travel, hospitality
 - Certain reasonable and bona fide promotional expenses ok
 - Goods or services for personal use
 - Cash
 - Commission
 - Employment offers, phony jobs or 'consulting' relationships
 - Kickbacks
 - Political and charitable contributions
 - Unexplained discounts or rebates
- Recordkeeping Requirements
- Criminal/Civil Penalties for Bribery or failure to maintain proper records

Anti-Corruption Fundamentals

Focus on Foreign Government Officials

- Anti-corruption laws and enforcement focus on the bribing of government officials, broadly defined
- Caution should be taken when:
 - Selling to, or
 - Entertaining, or
 - Obtaining licenses or permits from **government officials**
 - Engaging in joint activities with foreign institutions
- Seek advice before
 - Paying expenses for, or
 - Giving contracts to or partnering with **government officials or relatives**

Anti-Corruption Fundamentals

Who is a Foreign Government Official

- An officer or employee, regardless of rank, of any national, provincial, or local government, including its departments, agencies and other government funded or owned bodies
- An officer or employee of a public international organization (e.g., the World Bank or the United Nations)
- An officer or employee of a political party or any party official
- A candidate for political office
- An officer or employee of a political party or any party official

Anti-Corruption Fundamentals

Who Could be Considered a Foreign Government Official?

- Hospital doctors and college administrators if hospital, college or other institution is government affiliated
- The head of trading from a Bank if the government owns or controls all or a portion of the Bank
- Employee of a corporation if the government owns or controls all or a portion of the corporation
- A retired professor of economics, if that professor is acting as an official advisor to the government
- A consultant you have engaged to help you determine your product strategy, if that consultant has a 'day job' working in any capacity for the government
- A princess, or other members of a royal family
- A close relative to any of the above (e.g., spouse, sibling or child)

Anti-Corruption Fundamentals

Liability for Acts of Intermediaries/Consultants/Agents

- You may be liable for the acts of your intermediaries if you '**know**' that your intermediary is or is likely to pay a bribe
- You will be treated as '**knowing**' that your intermediary might pay a bribe if you have:
 - Actual knowledge; or
 - Firm belief that prohibited payment is likely to occur; or
 - Awareness of high probability of prohibited payment; or
 - You can be shown to have ignored obvious warning signs
- Knowing includes **conscious disregard** or **deliberate ignorance**
- Must conduct due diligence

Anti-Corruption Fundamentals

Red Flags for Intermediaries/Consultants/Agents

- Intermediary has **reputation** for unethical conduct
- Unusual methods of payment: payments to be made in cash, in goods and services, **via another person** or entity or into a third-country bank account
- Intermediary provides invoices that lack detail or description doesn't match services
- Requests for money to '**get the business**' or 'make the necessary arrangements'
- Intermediary insists on **anonymity**
- Intermediary was recommended by or has ties to a **government official**
- Intermediary doesn't have the necessary staff, facilities, or expertise to perform the services
- Intermediary is uncooperative during an **audit** or **due diligence**
- History of corruption in country

High Profile Enforcement

- **Siemens** – December 15, 2008 – Pleaded Guilty and Criminal and Civil Fines of \$1.6 Billion to U.S. and Germany
 - internal independent compliance monitor imposed
 - \$1 Billion in investigative costs
- **Halliburton/Kellogg Brown & Root** – February 11, 2009 – Pleaded Guilty to FCPA Violations and \$579 Million in Criminal and Civil Fines
- **BAE Systems** – March 1, 2010 – Pleaded Guilty to FCPA Violations - \$400 Million Fine
 - internal independent compliance monitors imposed
 - Executives detained at U.S. airports
- **Daimler AG** – April 1, 2010 – Pleaded Guilty to FCPA Violations and \$185 Million in Criminal and Civil Fines
 - payments to officials in 22 countries
 - internal independent compliance monitor imposed
 - \$500 million in investigative costs
- **Rio Tinto** – China – March 2010
 - Australian employees of Rio Tinto sentenced to 7 to 14 years in jail in China

Recent Developments

- 2011 DOJ/SEC fines of \$650 million
- 2010 fines of \$1.8 billion
- Many fines as a result of self-disclosure
- Continued emphasis on prosecution of individuals
 - Record jail sentences
 - 15 years and 7 years in Haiti Teleco case
- Government losses in prosecution of individuals
 - Prosecutorial misconduct
- Increased use of non-prosecution or deferred prosecution agreements
- New whistleblower provisions
- Court decisions on foreign instrumentality/foreign official
 - Still unclear
 - Very fact intensive

THE COMMON LAW IS THE WILL OF *Mankind* ISSUING FROM THE *Life* OF THE *People*



THE UNITED STATES
DEPARTMENT OF JUSTICE

JUSTICE NEWS

Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, October 25, 2011

Executive Sentenced to 15 Years in Prison for Scheme to Bribe Officials at State-Owned Telecommunications Company in Haiti

Longest Prison Term Ever Imposed in an FCPA Case

WASHINGTON – The former president of Terra Telecommunications Corp. was sentenced today to 15 years in prison for his role in a scheme to pay bribes to Haitian government officials at Telecommunications D’Haiti S.A.M. (Haiti Teleco), a state-owned telecommunications company. This is the longest sentence ever imposed in a case involving the Foreign Corrupt Practices Act (FCPA). The former executive vice president of Terra was also sentenced today to 84 months in prison for his role in the bribery scheme.

The sentences were announced by Assistant Attorney General Lanny A. Breuer of the Justice Department’s Criminal Division; U.S. Attorney Wifredo A. Ferrer for the Southern District of Florida; and Special Agent in Charge Jose A. Gonzalez of Internal Revenue Service, Criminal Investigation Division (IRS-CID), Miami Field Office.

Joel Esquenazi, 52, of Miami, and Carlos Rodriguez, 55, of Davie, Fla., were sentenced by U.S. District Judge Jose E. Martinez in the Southern District of Florida. Judge Martinez also ordered the defendants to forfeit \$3.09 million.

Esquenazi and Rodriguez were convicted in August 2011 of one count of conspiracy to violate the FCPA and wire fraud; seven counts of FCPA violations; one count of money laundering conspiracy; and 12 counts of money laundering.

Recent Developments (continued)

- Huge internal investigative costs
 - Avon - \$93 million in 2011, \$95 million in 2010 and \$59 million in 2009
 - Loss of key executives
 - Takeover target
- Use of broader U.S. statutes
 - Travel Act
 - Wire fraud
 - Money laundering
 - Antitrust
- Increased focus on travel and entertainment
- Liability for pre-closing activities of acquired entity
 - Successor liability
- Conscious avoidance/should have known enough for criminal conviction

Recent Developments (continued)

- Shareholder private actions
 - Avon massive class action naming officers and directors
 - Wrongful termination case by Director of Global Compliance allegedly fired after Avon refused to implement FCPA compliance controls
 - Wynn Resorts class action naming directors
 - \$135 million donation to University of Macau, China
- Suits by competitors under antitrust laws for conspiracy
- Suits by foreign government under RICO, etc.
- FCPA Insurance
- FCPA Reporting Center: "Our attorneys are currently representing whistleblowers throughout Europe, Asia, Africa and North America. Call 1-800-934-2921 for a free no obligation consultation with a lawyer."

World Wide Enforcement

- UK Bribery Act
 - Bans all bribery
 - Bans facilitation payments
 - 3 year sentence imposed on British court clerk for fixing driving convictions
- New Chinese Anti-Bribery Law
 - Applies to all natural persons in PRC regardless of nationality and all companies registered under PRC law
 - New enforcement in China
- World Bank
 - Debarred 63 firms in 28 countries in FY 2012
- New Russia Anti-Bribery Law – fines and imprisonment

Clarifications/Guidance

- Congressional hearings and business requests
- Foreign official/instrumentality
- Compliance defense to FCPA
- Successor liability – guidance of what pre-acquisition due diligence is adequate
- Clear guidance on de minimis gifts and hospitality
- DOJ to provide new guidance in 2012

FCPA Plus – The Travel Act And More

- Travel Act, 18 U.S.C. § 1952
- Crime to travel or use mail or any other facility in interstate/foreign commerce to promote, manage, establish, carry on or facilitate promotion, management, establishment or carrying on of any unlawful activity
 - Including extortion and bribery in violation of laws of the state in which committed or of the United States

FCPA Plus – The Travel Act And More (continued)

- Advantages for Prosecution
 - Avoids ambiguous foreign official issues
 - Incorporates states' commercial bribery laws
- Forum shopping
- Expands scope of a conspiracy charge under 18 U.S.C. § 371
- U.S. v. Control Components Inc.
- Wire fraud
- Money laundering
- Antitrust laws

High Risk Areas

- New Employees (personal welcome and “reminder”) – Immediate training
- New Acquisitions – Instill Culture of Compliance
- Joint Ventures
- Third Parties/Agents/Intermediaries
- Countries with reputation for corruption
- Ambiguity on foreign official/instrumentality
- Selective prosecution/regime change
- Competitor Reporting

Best Practices

- Tone and action at Top – Set example
- Tone and action of mid-level managers
 - Where the action is
 - Buy-in of mid-level essential
 - Set right example
- Zero Tolerance
 - Small payments can start huge investigation
- Emphasize protecting company reputation earned over many years
- Training in person/face-to-face most effective
 - Employees open up
- Visits from headquarters to show importance
- Establish rapport/relationship
 - Door always open
- Keep it Simple

Best Practices (continued)

- Due Diligence of third parties/partners/acquisitions
- Native Language
 - Don't assume know English
- Reinforce at regular meetings/conference calls
- Advance preparation
 - Review documents
- Routine Audits
- Scrutinize expense reports
- Not Americanized – customize to country and activities
- Keep records of compliance training
- Impose consequences
- On-line training
- On-line reminders
- Use social media

Best Practices (continued)

- Focus on high risk areas and issues
- Emphasize competitive advantage
- Show policies of customers/competitors
- Periodic and regular compliance training
- Explicit prohibition of commercial bribery
- Describe what is permissible
- Multiple signatures/approval for transactions above certain amount
- Require third parties to certify compliance in writing, right to audit, and require they conduct compliance training
- Due diligence of third parties – document and update
- Emphasize government aggressiveness
 - Stings, recordings, wiretaps, informants, ambush interviews

Best Practices (continued)

- Update compliance materials
- Make sure compliance materials are readable
- Training on how to respond to ambush interview, search warrant, dawn raid, subpoena
- Effective internal reporting program – hot line
- Investigate quickly – Whistleblower bounty
- Important – seek legal advice
- Avoid appearance of impropriety
- Careful on what is written and said

Government and Internal Investigations

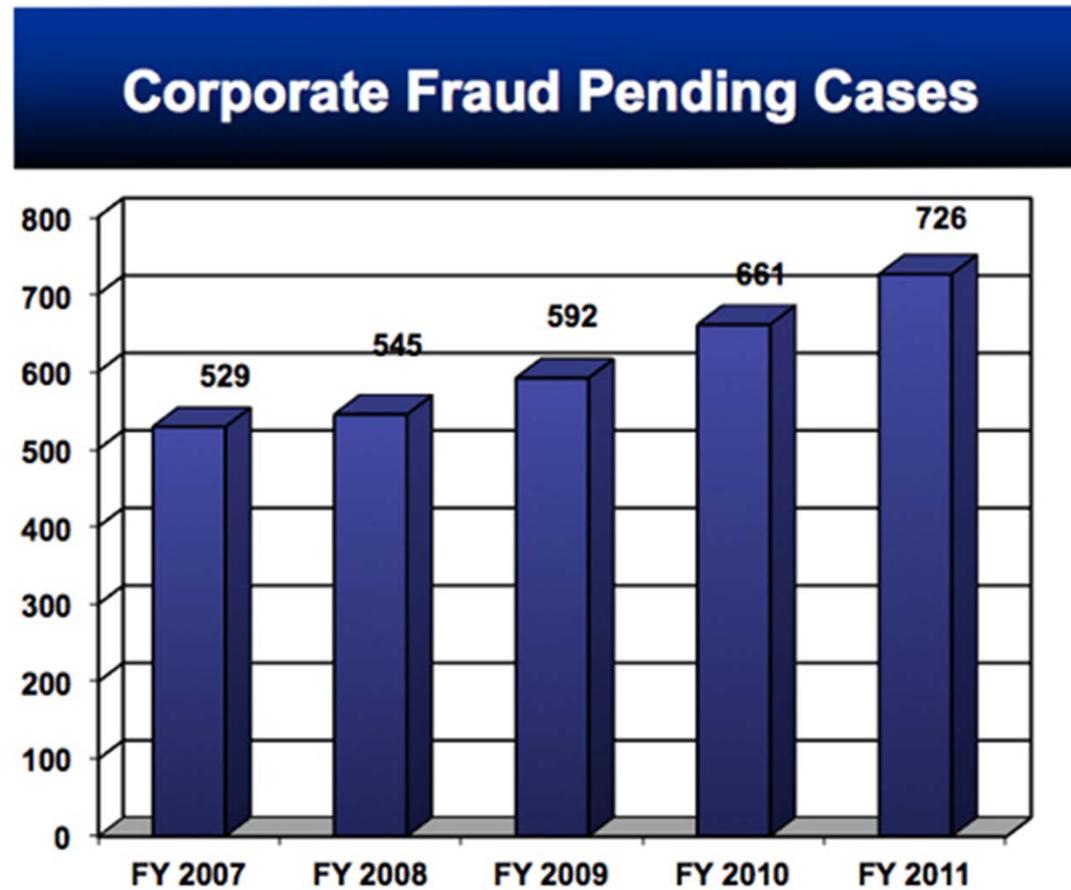
**Gary C. Shockley – Chair, Government
Regulatory Actions Group; Shareholder
Baker Donelson/Nashville**

**David McMahan – AVP/Regional Manager
Chartis/Atlanta**

**Scott Hilsen – Director
KPMG/Atlanta**

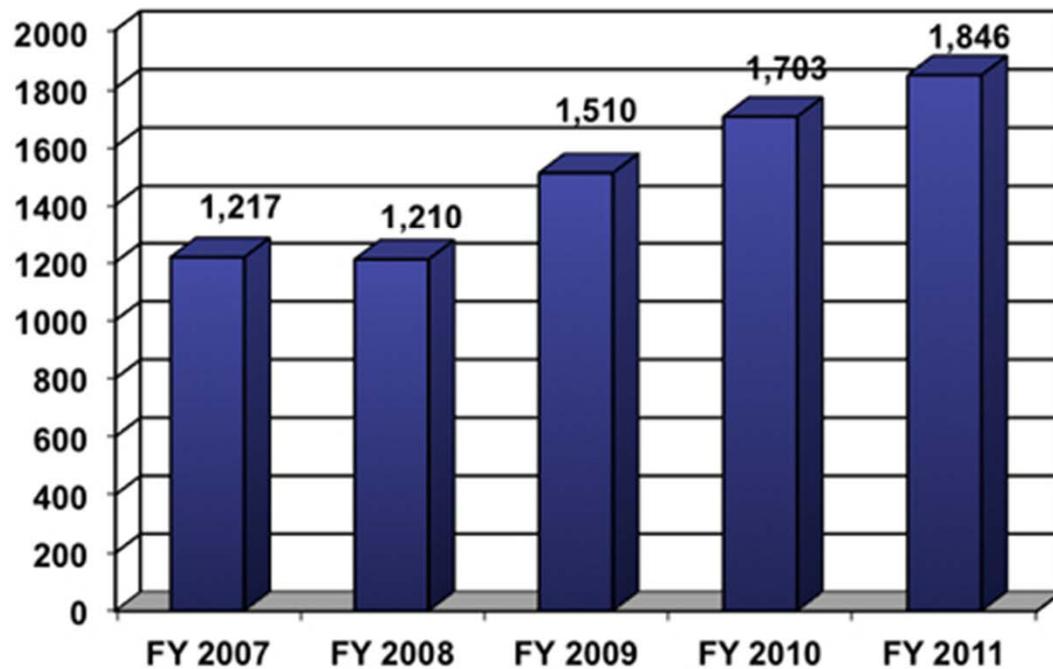
Government Investigations: What's Hot?

Source: FBI, Financial Crimes Report to the Public, FY2010-11



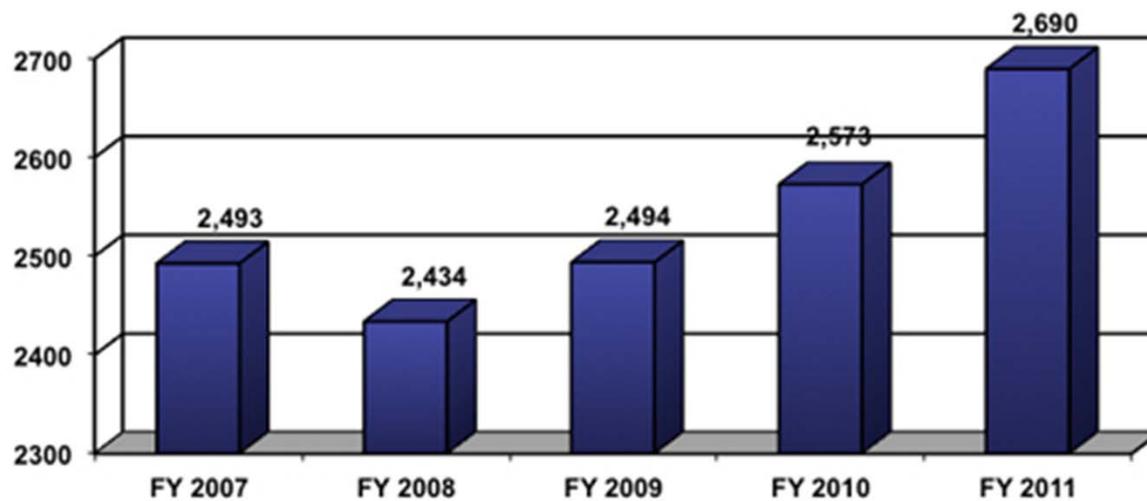
Government Investigations: What's Hot?

Securities and Commodities Fraud Pending Cases

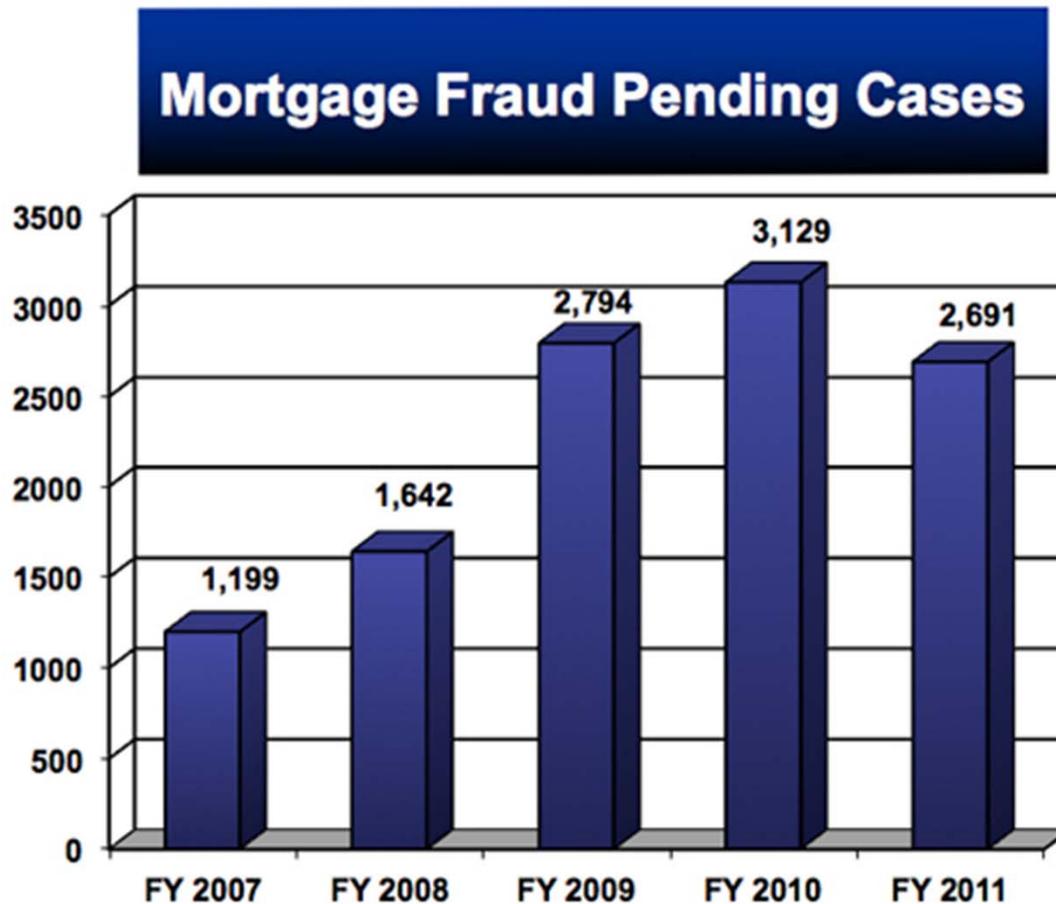


Government Investigations: What's Hot?

Health Care Fraud Pending Cases

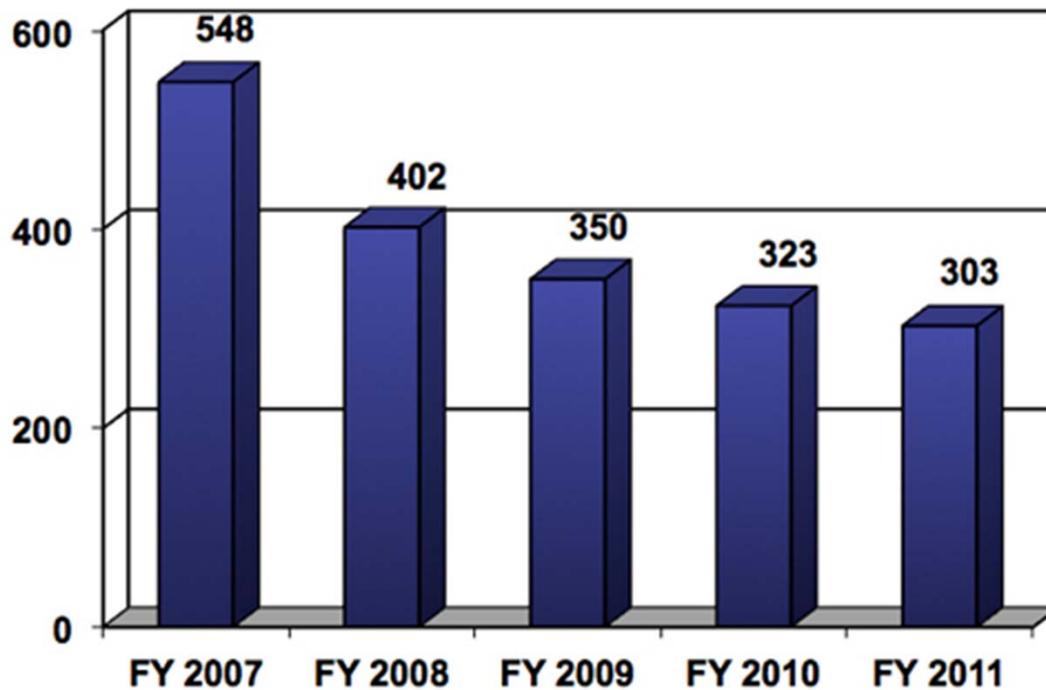


Government Investigations: What's Hot?



Government Investigations: What's Hot?

Money Laundering Pending Cases



Triggers for Internal Investigations

- Search warrant
- Grand jury subpoena (company or third parties)
- Letter of inquiry
- Congressional committee investigation
- Civil litigation, e.g., FCA, derivative, Title VII, retaliation
- Whistleblower tip to compliance hotline
- Press reports or inquiries
- Competitor problems
- Examples: *Woodmen of the World Life Ins. Soc. v. U.S. Bank N.A.*, No. 8:09CV407 (D. Neb. Feb. 2, 2012)(improper allocation of investment opportunities)

Attorney Client Privilege and Work Product Concerns in Internal Investigations

- Whose privilege is it, anyway?
- Legal versus business advice or investigative services
- Inside versus outside counsel
- Accountants, consultants, investigators and other non-attorneys
- Former employees
- Non-employees
- *Facts* versus communications
- Reports, interview memos, transcripts, advice
- Waiver: Intentional or inadvertent
- AWP and the substantial need and hardship test
- Examples: *In re Google, Inc.*, 2012 WL 371913 (Fed. Cir. Feb. 6, 2012) (e-mail from engineer re Oracle infringement claim)

Potential ESI Issues in Internal Investigations

- Litigation versus investigation holds
- Preservation in place versus forensic duplication
- Vendors versus in-house IT support
- Who's in and who's out of the investigation hold
- Avoiding opportunities for mischief
- The new SOX obstruction offense, 18 U.S.C. § 1519, and *U.S. v. Kernell*, 667 F.3d 747 (6th Cir. 2012)
- 3d Chess: Mobile devices, social media, cloud computing, state and international privacy restrictions
- Examples: Fed. R. Evid. 502

Incentives for Investigation and Disclosure

- DOJ Antitrust Division Corporate Leniency Policy (8/10/93), Individual Leniency Policy (8/10/94)
- DOJ McNulty Memo (Dec. 2006)
- SEC Enforcement Cooperation Initiative: Individual Policy Statement (Jan. 19, 2010), Seaboard Report
- EPA Incentives for Self-Policing (April 11, 2000)
- TDEC Policy Encouraging Self-Policing and Voluntary Correction (May 11, 2000)
- U. S. Sentencing Guidelines: Sentencing of Organizations §§ 8B2.1 (compliance and ethics program), 8C2.5(f) & (g) (credit for compliance program and voluntary disclosure in culpability score)
- Example: Smith & Nephew Deferred Prosecution Agreement (Feb. 2012)

The Warren Commission Report: Lessons for Corporate Internal Investigations



The Warren Commission Report: Lessons for Corporate Internal Investigations

- Who
 - Too close to those being investigated
- Cooperation
 - Not told of Operation Mongoose, FBI contacts with Oswald
- When
 - “Rush to judgment,” pressure from LBJ (11/29/63-9/24/64)
- Depth and plausibility
 - The “magic bullet,” timing of the three shots, Grassy Knoll
- Inherent limitations in available evidence
 - Oswald, autopsy from Walter Reed, audio tapes (available to House Committee)
- Public Perceptions

Recent Decisions of Interest

- *Kozlowski v. Hulihan*, No. 09 Civ. 7583 (S.D. N.Y. Feb. 7, 2012)(former CEO and CFO of Tyco waived issues regarding discovery of internal investigation's interviews of directors by failing to object at state court trial)
- *U.S. v. The Williams Cos.*, 562 F.3d 387 (D.C. Cir. 2009)(waiver)
- *Reitz v. City of Mt. Juliet*, 680 F.Supp.2d 888 (M.D. Tenn. 2010) (waiver by assertion of *Farragher-Elleerth* defense)
- *Woodmen of the World Life Ins. Society v. U.S. Bank, N.A.*, No. 8:09CV407 (D. Neb. Feb. 2, 2012)(waiver by disclosure to SEC)
- *U.S. v. Gray*, 642 F.3d 371 (2d Cir. 2011)(false statement to private corrections contractor supported false statement convictions)
- *U.S. v. Hanna*, 661 F.3d 271 (6th Cir. 2011)(exclusion of testimony by general counsel of competitor re findings of internal investigation on shipments to Iraq)

Recent Decisions of Interest

- *U.S. v. Yielding*, 657 F.3d 688 (8th Cir. 2011)(hospital discovered and disclosed kickback scheme through investigation of missing bone and excess inventory of bone growth stimulators)
- *U.S. v. Reyes*, 660 F.3d 454 (9th Cir. 2011)(testimony of corporation's former general counsel re statement by CEO on backdating stock options was relevant to rebut CEO's trial defense)
- *In re Google, Inc.*, 2012 WL 371913 (Fed. Cir. Feb. 6, 2012) (e-mail from engineer to head of Android operations regarding alternatives to Java were not part of counsel's investigation of Oracle infringement claim; inclusion of "Google Confidential" and "attorney work product" notations and CC of corporation's senior counsel did not preclude production)

Contact Information

Baker Donelson

- John Calender jcalender@bakerdonelson.com
- Tonya Grindon tgrindon@bakerdonelson.com
- Scott Sherman ssherman@bakerdonelson.com
- Gary Shockley gshockley@bakerdonelson.com
- Matt Sweeney msweeney@bakerdonelson.com
- Steve Wood sfwood@bakerdonelson.com

Chartis

- David McMahan david.mcmahan@chartisinsurance.com

KPMG

- Scott Hilsen shilsen@kpmg.com

BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

Thanks!

BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

CHARTIS 



EXPAND YOUR EXPECTATIONSSM