MARSH

LEADERSHIP, KNOWLEDGE, SOLUTIONS...WORLDWIDE.

Expanding Areas of Liability for Insurers and Insureds

July 15, 2015

MARSH & McLENNAN COMPANIES

Welcome to Marsh's 2015 Insurance Company Conference

Deborah Lodge

- Partner, Squire Patton Boggs
- Specializes in intellectual property, privacy and Internet law.

Samuel Rosenthal

- Partner, Squire Patton Boggs
- Leads Government Investigations and White Collar Practice Group.

Steve McHale

- Partner, Squire Patton Boggs
- Advises businesses on issues of national security law and policy.

Agenda

- Cybersecurity
- Recent Developments in Corporate Governance
- Sanctions
- Questions and Answers

The Cybersecurity Perspective

- The Changing Nature of the Threat Environment: Economic and National Security.
- Who is at Risk?
- Cost of Cybersecurity.
- Issue: Not IF a company will suffer a breach, but WHEN.
- “Why Cybersecurity Leadership Must Start At The Top”
  - http://www.forbes.com/sites/frontline/2015/07/13/why-cybersecurity-leadership-must-start-at-the-top/ -- July 13, 2015.
- Governmental Priority: Presidential Executive Order on Cybersecurity, Critical Infrastructure.

Cost of Cybersecurity

- $11.6 million = Average cost per company per cyber attack in 2013 (Ponemon Institute).
- $32,469 = Average cost per day to a company as it resolves a cyber attack (Ponemon Institute).
- 32 = Average number of days it takes a company to resolve a cyber incident in 2014 (Ponemon Institute).
- $400 billion = Estimated cost of cyber crime worldwide per year (Center for Strategic and International Studies).
- 200,000 = Number of US jobs impacted by cyber crime (Center for Strategic and International Studies).

Why Is Cybersecurity A Hot Button Issue?

- Cybersecurity is a core area of concern for all companies.
- Due to potential risk and liability, cybersecurity is a matter for boards and C-suites, not just compliance and IT departments.
  - Cyber Breach claims in 2013 ranged from $2,500 to $20 million.
  - Median claim pay out by insurers in US was $250,000.
  - Median cost for crisis services (legal, forensics, notification) was $210,000.
  - Emerging standards of care for Directors and Officers.
- Corporate silos mean many companies are at risk.

Top Threat to Economic and National Security

- Several Obama Administration officials have testified before a number of Congressional Committees and named cybersecurity as the top threat to US national security.
  - Director of National Intelligence James Clapper.
  - Federal Bureau of Investigation Director James Comey.
  - Former Director of the National Security Agency and Commander of US Cyber Command Keith Alexander.

Executive Order -- Improving Critical Infrastructure Cybersecurity – February 12, 2013

- It directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure.
- NIST: National Institute of Standards and Technology.
- Part of the Department of Commerce.
- Lead role in cybersecurity standards.
- Framework for Improving Critical Infrastructure Cybersecurity.
  - February 2014.
  - standards, guidelines, and practices to promote the protection of critical infrastructure.
  - developed through collaboration between industry and government.

Critical Infrastructure Sectors, per Executive Order

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- **Financial Services**
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

Office of Personnel Management Hacked

- In April 2015, OPM discovered that the **personnel data of 4.2 million current and former Federal government employees had been stolen.**
- In early June 2015, OPM discovered that, actually, personal data of 21.5 million Federal government employees, job applicants and contractors had been compromised: including **background investigation records of current, former, and prospective Federal employees and contractors.**

Aftermath Of A Data Breach

- Internal Investigations and Fixes.
- Reports to Government Authorities.
- Notice to Affected Persons/entities.
- Regulatory investigations: FTC, SEC, CFPB, Attorneys General.
- Lawsuits.
  - Against company, by consumers, financial institutions.
  - Shareholder derivative cases and securities class actions.
  - Shareholder actions against directors and officers.
    - Alleging claims for breach of fiduciary duty and/or securities fraud.

Consequences of Cybersecurity Breaches

- Severe decline in stock prices following announcement.
- Decreased Customer Loyalty.
- Negative Publicity.
- Costs of Remediation, Upgrades, Customer Anti-Identity Theft Protection.

D&O Exposure For Cybersecurity Failures – Securities Class Actions

- In re Heartland Payment Systems, Inc.
  (Civ. No. 09-1043, U.S. District Court, District of New Jersey)
  - Related to 2008 breach: 100 million debit/credit card numbers stolen
  - Class actions were filed on behalf of financial institutions, cardholders, and stockholders
  - Stock price plunged 50% within days
  - Securities Action alleged false statements in 10-K
    - that Heartland “place[d] significant emphasis on maintaining a high level of security”
    - Court: dismissed investor suit. 10-K did not say Heartland was immune from security breaches
  - Consumer class action settled: Heartland agreed to pay anyone who could damages due to identity theft or fraud. Received 290 consumer claims; only 11 were found to be valid. $1975 total.

Shareholder Derivative Actions Against D&Os

- Becoming more popular.
- Typically tag along with securities fraud class actions.
- Pre-suit shareholder demand letters to review documents.
- Pre-suit demand letters.
  - Special Litigation Committees.
- Significant defense costs to defendants at motion to dismiss stage.

Shareholder Derivative Actions Against D&Os

- Wyndham Worldwide Corporation Litigation – Palkon v. Holmes, Case No. 2:14-cv-01234 (D.N.J.)
  - After FTC lawsuit asserting unfair and deceptive acts due to breaches.
  - Breach of fiduciary duty for failure to implement adequate security measures; failure to have adequate cybersecurity measures caused shareholders to suffer the damages of the FTC investigation and case.
  - Claimed D&O's knew system was vulnerable to breach due to outmoded data systems.
  - Waste of corporate assets by failing to implement adequate internal controls to prevent breaches.
  - Wrongfully rejected pre-suit demand argument.
  - October 2014: Shareholder suit dismissed.
    - Business judgment rule.
    - Facts showed Board tried to deal with data security problems.

Shareholder Derivative Actions Against D&Os

- Target Corporation Derivative Litigation – 2014 (D. Minn.)
  - Similar to Wyndham complaint
  - Breach of fiduciary duty for failure to implement appropriate internal controls to protect customer data, detect and prevent breaches and timely report
  - Privacy Policy: Target will “maintain administrative, technical and physical safeguards to protect your personal information”
  - 10-K Risk disclosure: Target was aware of risks
  - Lost revenue and profits due to loss of customer confidence
  - Costs of investigations and settlements
  - Credit downgrades

Shareholder Derivative Actions Against D&Os

- NIST Cybersecurity Framework will serve plaintiff as establishing parameters of standard of care.
- FTC enforcement gives added weight.
  - Wyndham case: Failure to have adequate data security is “unfair practice”.
  - Deceptive practice if privacy statements not accurate, not followed.
- State statutes will also serve plaintiffs.
  - Florida Information Protection Act.
  - Attorney General actions will provide examples of what conduct is “reasonable”.
  - States are increasingly passing their own cybersecurity laws.

How Have Duties of D&Os Changed in the Cyber World?

- Data privacy and data security must be a priority.
  - On the regular meeting agenda.
  - Ensuring adequate resources are devoted to data privacy and data security.
  - Designating a Board Committee to oversee and report to Board.
  - Bring the CTO or CIO out of the data-basement.
- Anticipate issues.
  - Retain outside experts to review system.
  - Address any issues or deficiencies.
  - Have Crisis Response Team in place: with legal, IT, PR, and other personnel, ready to investigate and respond to any data breach issue.
- Document Actions and Progress.
  - Directors and Officers must demonstrate their diligence and good faith.
  - Review risk disclosures and security status with care.

Regulatory Liability and Consequences

Directors, Officers, Employees Face:

- Criminal Prosecution.
- Cease & Desist Orders.
- Civil Money Penalties.
- Shareholder derivative suits.
- Removal/Prohibition Orders.
- Restitution Orders for losses or unjust enrichment.

SEC: securities violations and FCPA

Another core principle of any strong enforcement program is to pursue responsible individuals wherever possible. That is something our enforcement division has always done and will continue to do. Companies, after all, act through their people. And when we can identify those people, settling only with the company may not be sufficient. Redress for wrongdoing must never be seen as "a cost of doing business" made good by cutting a corporate check.

SEC Chairwomen

Mary Jo White

OCC:

"We believe at the OCC that you need to hold CEOs and the boards of directors accountable for BSA/AML policies and procedures and their compliance program."

"We are looking at our authority under Section 8 of the FDIC Act to actually remove from office or prohibit from banking those individuals that violate BSA programs. So we are looking to try to tighten up the legal duties and authorities of individuals at banks and then to enable us to take an appropriate level at the civil, administrative level, and potentially to assist the criminal authorities."

OCC Chairman Curry

Chairman Tim Johnson (D – SD)

- **Chairman's opening remarks:**

"The government depends on bank compliance programs to detect and prevent money laundering... And [as] the recent major penalty cases [show], U.S. banks failed to deal effectively with funds from non-U.S. banks or affiliates... How can we ensure uniform compliance and enforcement of U.S. and international rules?"

"We should consider today the full range of remedies in cases like these including BSA injunctions from the industry [for] those individuals who violate the rules..."

Are regulators focused only on large banks?

- **Testimony of the Comptroller, Tom Curry:**

"Although many of our recent enforcement actions have involved large banks, BSA is an issue for institutions of all sizes. In fact, as large banks improve their BSA/AML programs and jettison higher risk lines of business, we are concerned that money-launderers will migrate to smaller institutions."

Increased Attention on Management

"We believe at the OCC that you need to hold CEOs and the boards of directors accountable for BSA/AML policies and procedures and their compliance program."

"Most of the problems we find in BSA/AML programs are attributable to the following root causes:

- the strength of an institution's compliance culture;
- its willingness to commit sufficient resources;
- the strength of its information technology and monitoring processes; and
- its risk management.

The health of a bank's culture starts at the top. And so it's important that senior management demonstrate a commitment to BSA/AML compliance. Employees need to know BSA compliance is a management priority and that the compliance function will receive the resources it needs to succeed, including training and first-rate information technology."

Hearing testimony of the Comptroller.

Health Care

- DOJ invigorating the Health Care Fraud Unit with 40 new prosecutors:
  - “the largest and most prolific unit of criminal prosecutors dedicated solely to health care fraud in the country.”
- Convictions of Executives in the Peanut Corp. of America case.

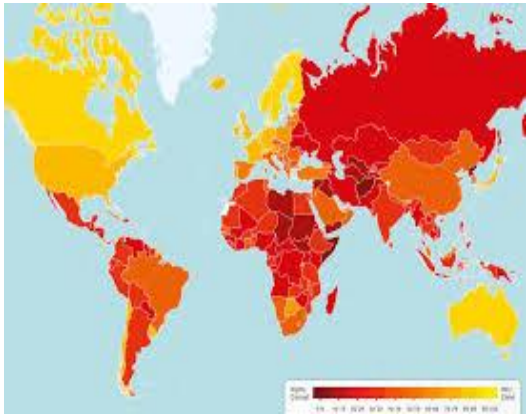
The common theme?

- Lack of internal controls
  - JPMC Bank, N.A., Columbus, Ohio (January 2013):
    - Insufficient internal controls, independent testing, customer due diligence, risk assessment, and reporting suspicious transactions.
    - Lack of enterprise-wide policies and procedures to ensure foreign branch suspicious activity.
    - Lack of enterprise-wide policies and procedures to ensure that, on a risk basis, customer transactions at foreign branches were assessed, aggregated, and monitored.

Added vulnerabilities and therefore enhanced duty of care:

Foreign operations.

- JPMC Case:
  - Lack of enterprise-wide policies and procedures to customer transactions at foreign branches were assessed, aggregated, and monitored.
  - **And particularly in problem jurisdictions:**



SEC

‘‘[B]oards that choose to ignore, or minimize, the importance of cybersecurity responsibility do so at their own peril.’’

Luis A. Aguilar, SEC Commissioner

Problem customers, partners or affiliates?

- Five Directors & Executive Officers of Security Bank, N.A., *North Lauderdale, Florida* (January 2013)
  - 2010 C&D Order.
  - Directors approved appointment of Secretary of Board who previously had been convicted of tax evasion, a violation of 12 U.S.C. § 1829.
  - Former CEO brought high risk business to Bank knowing it was ill-equipped to monitor and control the accounts.

New untested products?

- First Bank of Delaware, Wilmington (November 2012) ($15 Mill. Penalty):
  - Bank failed to adequately oversee MSB and third party payment processor relationships and related programs (e-payments) and services.
  - “To make money, First Bank of Delaware entered into risky lines of business . . . As a result of its failure to implement systems and controls to identify and report suspicious activities, as required by the BSA, financial predators were able to victimize consumers.”
- JPMC:
  - consent order required review of new products and services under a high level of compliance review for new products and services.

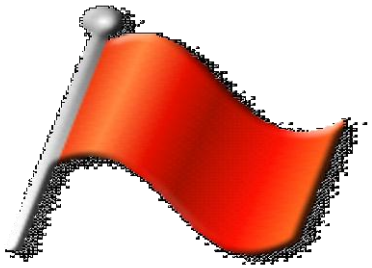
Proposed Legislation

Proposed legislation would add the following to existing laws:

- Heavier civil money penalties.
- Penalties for mere negligence.
- Executive Branch must justify light treatment.
- Clawback of compensation for executives.
  - “Removal and prohibition” of individuals from operating in the industry.
- Whistleblower protections extended to the financial industry.

FINRA Enforcement Actions

- FINRA Rule 3310 (2002) - minimum standards for AML compliance programs for broker-dealers consistent with BSA: follows four pillars.
- FINRA stepping up enforcement of AML violations:
  - in 2012, 49 enforcement actions against broker-dealers for AML violations.
  - reflects a 36% increase from the 36 AML-related cases concluded in 2011.



New Enforcement Mechanism at OCC

- Major Matters Supervision Review Committee
  - established by the Comptroller in late 2012 to review all large bank enforcement actions including BSA violations, BSA CMPs involving large banks, and all prohibitions/removals against individuals for BSA violations.
  - five members chaired by OCC's Senior Deputy Comptroller for Bank Supervision Policy and Chief National Bank Examiner (currently, John C. Lyons).
  - other members include: the Chief of Staff; the Senior Deputy Comptrollers for Bank Supervision Policy and Community Bank and Large Bank Supervision; and the Chief Counsel.

New Guidelines Forthcoming on Corporate Governance Impacting BSA/AML Compliance

"The OCC is in the process of drafting detailed guidance to banks on sound corporate governance processes... including business line accountability for BSA/AML compliance and the independence of the compliance function."

Written Testimony of the Comptroller.

Sanctions

- Part 1: Trending Now.
  - Russia/Ukraine Sanctions.
  - Iran.
  - Syria & Sudan.
  - Cuba.

- Part 2: Tips for Insurers and Reinsurers.

- Part 3: What is next?

Russia

- Russian sanctions are complicated.
- Over 100 individuals and entities blocked.
- New type of sanctions: Sectoral sanctions.
  - US and EU persons prohibited in dealing in equity or debt of more than 30-days maturity of certain large Russian banks.
  - US and EU persons cannot not deal in anything but short-term debt of most major Russian energy and defense companies.
  - Limits on activities in support of Arctic, offshore and shale formation energy production.

Crimea

- Designation of individuals and political entities **undermining the sovereignty and territorial integrity of Crimea.**
- Exports to or imports from Crimea (including services) prohibited.
- Designation of a Crimean-based energy company that received the expropriated assets of a Ukrainian state-owned company.
- Designation of Russian bank that took over branches and business of expropriated Crimean bank.

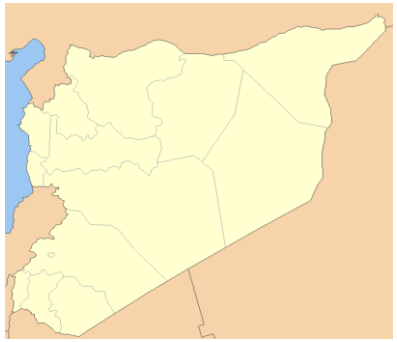
Russia: What Does This Mean For (Re)insurers?

- Higher risk insuring business involving Russian energy sector.
  - Need to know what is being provided or what work is being done.
  - Need to know where the project is located.
  - Need to know end user and end use.
  - Need to make sure that insureds have programs to prevent diversion.
- Can not engage in any business, direct or indirect, with SDN banks or any other SDNs.
- No prohibition on doing business with SSI banks, except if it involves new equity or debt issued by those banks.
- Higher risk insuring business with Russian defense sector.
- No business involving Crimea in any way.
  - **If things get worse, sanctions will get tougher.**

Iran

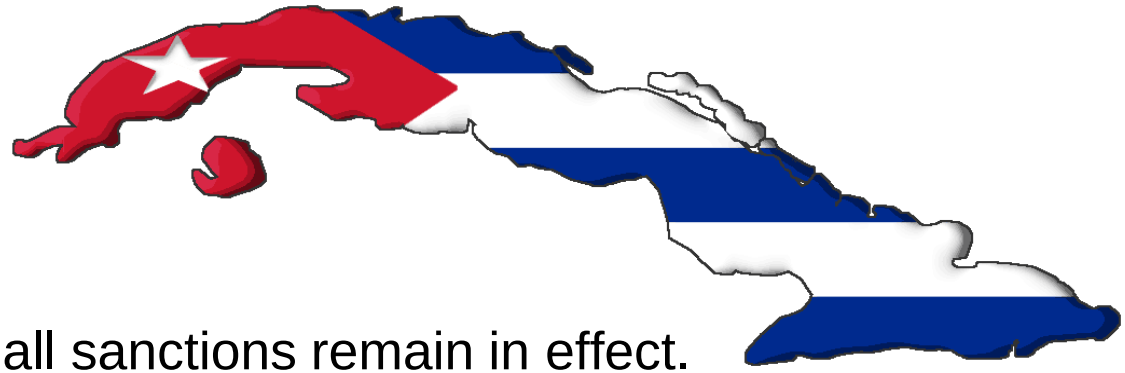
- End of Sanctions? Maybe/Maybe not.
  - End of nuclear proliferation sanctions.
  - BUT Iran would still be a “State Sponsor of Terrorism”.
- Not now anyway.
  - President can waive many of the sanctions.
  - BUT Congress gets 60 days to review first.
  - Treasury says all sanctions remain in place for now.
  - UN Security Counsel must endorse.
  - IAEA must verify Iranian compliance.
  - Timeline remains uncertain.
  - US persons likely to continue to face restrictions/EU probably few.
- Snap back.

Syria and Sudan



- No US company may extend coverage or pay a claim to anyone in Syria or Sudan.
- Or any sanctioned entity wherever located.

Cuba



- Almost all sanctions remain in effect.
- Still apply to foreign subsidiaries of US companies.
- If coverage is for a permitted transaction, get advice.
  - Travel insurance for authorized travel.
  - Global policies do not need Cuban exception.
- No sign that Congress has any interest in repealing sanctions.

General Pointers for (Re)Insurers

- US (re)insurers must comply with US sanctions.
  - Anywhere in the world.
  - Foreign subsidiaries generally not covered by US sanctions.
    - EXCEPT: Cuba.
    - No US person can facilitate prohibited transactions.
  - Non-US (re)insurers must comply with respect to operations in the US.
- US and EU increasingly adopt complementary sanctions regimes.

General Pointers for (Re)Insurers

- Protect against cover being extended to unknown persons or payments made to persons who are subject to US sanctions.
  - Due diligence: Need to know insured and beneficiaries.
  - Due diligence on all intermediaries.
  - Due diligence whenever there is going to be an assignment.
  - Repeat due diligence: Need to know who is being paid on the claim.
- Don’t just check the OFAC SDN list.
  - Check OFAC’s new SSI list and Foreign sanctions evaders lists.
  - Check EU list.
  - Better yet use a service that will automate the process and check multiple lists.
- Documentation.

General Pointers for (Re)Insurers

- Use sanctions exclusion clauses and warranties to mitigate sanctions risk.
  - exclude from cover any risk or activity that would violate US (and EU) sanctions.
  - exclude liability pay claims or other items including return premiums (or provide any other benefit under the (re)insurance contract concerned) which would breach sanctions laws.
  - BUT: Clauses do not offer full protection since extension of coverage itself can be a violation. Strict liability.

What is Next on Sanctions

- ?????

Q&A

Deborah M. Lodge

- 2550 M St., N.W.
- Washington, D.C. 20036
- (202) 457-6330

Samuel Rosenthal

- 2550 M St., N.W.
- Washington, D.C. 20036
- (202) 457-6321

Steve McHale

- 2550 M St., N.W.
- Washington, D.C. 20036
- (202) 457-6344.

Thank you for Attending

- E-mail FinancialInstitutions@marsh.com to receive a copy of the slides.
- A replay of this call will be available on Marsh.com later this week. You will receive a link to the replay and a survey.
- Marsh's 2016 Insurance Company Conference.
  - Q1 2016.
  - Watch your inbox for a Save the Date later this summer.