FRIDAY, FEBRUARY 27, 2015
CLE 9
2:00 p.m. – 3:30 p.m.

How Will Dodd-Frank Weather the Coming Storm?
How Will Dodd-Frank Weather the Coming Storm

NBA Commercial Law Section
CLE Presentation
February 27, 2015

National Bar Association’s Commercial Law Section
28th Annual Corporate Counsel Conference
Ritz-Carlton Golf Resort, 2600 Tiburón Drive, Naples, Florida
Overview

1. Objectives
2. The Dodd–Frank Wall Street Reform and Consumer Protection Act (Selected sections)
3. Fed Delays Volcker Rule, Again
4. Democrats Tell The SEC To Get Moving On CEO Pay Rule
5. High Frequency Trading & Securities Law
6. Cybersecurity and the Securities Markets
7. Enforcement Actions
   A. Insider Trading
   B. Private Equity Enforcement Action
8. Dodd-Frank & Law Practice
9. Next Steps
How Will Dodd-Frank Weather the Coming Storm

Objectives

This seminar will discuss the perspectives of securities law experts on the current state of US securities law and the impact of the changed political landscape impacting Dodd-Frank. This panel discussion will focus on recent changes resulting from Dodd-Frank including delays on the "Volcker Rule," challenges in passing the final rules on implementing a proposed CEO pay ratio, and the Department of Labor (DOL) proposed a change to the definition of fiduciary under the Employee Retirement Income Security Act (ERISA). The panel will also discuss securities law changes related to increased changes in technology such as the regulation of High Frequency Trading (HFT) and Cybersecurity in the financial industry protection. Case discussions will include recent Supreme Court and Federal Circuit decisions examining the bounds of enforcement powers over private equity firms and others in the capital markets.
The Dodd-Frank Act 2015

“it's Obamacare for banks.”
Rep. Paul Ryan (R-Wis.)
How Will Dodd-Frank Weather the Coming Storm

• The Dodd–Frank Wall Street Reform and Consumer Protection Act (Pub.L. 111–203, H.R. 4173; commonly referred to as Dodd-Frank) was signed into federal law by President Barack Obama on July 21, 2010 at the Ronald Reagan Building in Washington, DC.

• Passed as a response to the Great Recession, it brought the most significant changes to financial regulation in the United States since the regulatory reform that followed the Great Depression.

• Critics have attacked the law, some arguing it was not enough to prevent another financial crisis or more bailouts, and others arguing it went too far and unduly restricted financial institutions.

• On December 2, 2009, revised versions were introduced in the House of Representatives by then Financial Services Committee Chairman Barney Frank, and in the Senate Banking Committee by former Chairman Chris Dodd. Due to their involvement with the bill, the conference committee that reported on June 25, 2010 voted to name the bill after the two members of Congress.
Fed Delays Volcker Rule

- The Federal Reserve Board announced that it has acted under section 619 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, commonly known as the Volcker Rule, to give banking entities until July 21, 2016, to conform investments in and relationships with covered funds and foreign funds that were in place prior to December 31, 2013 ("legacy covered funds").

- The Board also announced its intention to act next year to grant banking entities an additional one-year extension of the conformance period until July 21, 2017, to conform ownership interests in and relationships with legacy covered funds.

- This extension would permit banking entities additional time to divest or conform only legacy covered fund investments. All investments and relationships in a covered fund made after December 31, 2013, must be in conformance with section 619 of the Dodd-Frank Act and implementing rule by July 21, 2015. This extension would not apply to proprietary trading activities, and banking entities must conform proprietary trading activities to the final rule by July 21, 2015.
Federal Reserve Further Delays Volcker Rule

• The Volker Rule generally prohibits insured depository institutions and any company affiliated with an insured depository institution from engaging in proprietary trading and from acquiring or retaining ownership interests in, sponsoring, or having certain relationships with a hedge fund or private equity fund. These prohibitions are subject to a number of statutory exemptions, restrictions, and definitions.

• The rules to adopt the Volker Rule (section 619) were implemented by the Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Securities and Exchange Commission, and the Commodity Futures Trading Commission in December 2013.
CEO Pay Ratio Rules

"While CEOs can create value for companies, so can ordinary workers.....Pay ratio disclosure helps investors evaluate the relative value a CEO creates, which facilitates better checks and balances against insiders paying themselves runaway compensation...."

- Sen. Robert Menendez (D-N.J.) organized a letter to SEC Chair Mary Jo White demanding action on the rule, 12/2014
SEC To Get Moving On CEO Pay Rule

- SEC Chair White has been widely criticized for being soft on corporate managers and failing to regulate dark money in the campaign finance system.

- The SEC proposed the CEO Pay rule in September 2013. The standard 60-day period for public comments expired in December of last year, but the agency has yet to implement the proposal.

- The 2010 Dodd-Frank financial reform law required the SEC to craft a CEO pay ratio rule. Companies have furiously lobbied the agency to delay or water down the proposal to allow calculation methods that would result in a lower ratio between CEOs and typical workers.
CYBERSECURITY AND THE SECURITIES MARKETS

- March 2014 SEC Roundtable
- Cybersecurity Landscape
- Public Company Disclosure
- Market Systems
- Broker-Dealers, Investment Advisers, and Transfer Agents
- OCIE Cybersecurity Initiative
- Importance of Cybersecurity in the Market System
- Initiative Objectives and Exam Focus
- Document and Information Requests
High Frequency Trading Enforcement Actions

• **Disclosure Violations and Regulatory Failures in Operating Dark Pool** SEC charged a subsidiary of UBS with disclosure failures and other securities law violations related to the operation and marketing of its dark pool. UBS Securities LLC agreed to settle the charges by paying more than $14.4 million, including a $12 million penalty that is the SEC’s largest against an alternative trading system (ATS). An SEC examination and investigation of UBS revealed that the firm failed to properly disclose to all subscribers the existence of an order type that it pitched almost exclusively to market makers and high-frequency trading firms. UBS consented to the SEC’s order without admitting or denying the findings. The order censures the firm and requires payment of $2,240,702.50 in disgorgement, $235,686.14 in prejudgment interest, and the $12 million penalty. *In the Matter of UBS Securities LLC, Adm. Proc. File No. 3-16338 (instituted January 15, 2015).*

• **BATS Global Markets** have agreed to pay a $14 million penalty to settle charges that their rules failed to accurately describe the order types being used on the exchanges. An SEC investigation found that while operating under rules that described a single “price sliding” process for handling buy or sell orders, the EDGA Exchange and EDGX Exchange actually offered three variations of “price sliding” order types. The SEC’s investigation further found that the exchanges separately disclosed information about how those order types operated to some but not all of their members. *In the Matter of EDGA Exchange, Inc., and EDGX Exchange, Inc., Adm. Proc. File No. 3-16332 (instituted January 12, 2015).*
Recent Enforcement Actions

- SEC Charges Four India-Based Brokerage Firms with Violating U.S. Registration Requirements – *In the Matter of Motilal Oswal Securities Limited, In the Matter of JM Financial Institutional, Ambit Capital Private Limited and Edelweiss Financial Services Limited*, – The firms agreed to pay more than $1.8 million combined to settle the SEC’s charges.

- *SEC v. Fabrizio Neves, et. al.* – SEC filed a civil fraud action against two former brokers in Miami for overcharging customers approximately $36 million by using hidden markup fees on structure note transactions.


- *SEC v. Peter Madoff* – SEC charged Peter Madoff, brother of Bernie Madoff with committing fraud, making false statements to regulators and falsifying books and records in order to create the false appearance.
Enforcement Actions; Insider Trading

- **SEC v. Thomas Conradt et al.** – SEC charged two retail brokers who formerly worked at a Connecticut based broker dealer with insider trading on non-public information ahead of IBM Corporations acquisition of SPSS Inc.

- **SEC v. John Lazorchaz, et. al.** – SEC charged three health care company employees and four others in a New Jersey-based insider trading ring of various high school friends generating $1.7 million in illegal profits and kickbacks by trading in advance of 11 public announcement involving mergers, a drug approval application, an quarterly earnings of pharmaceutical companies and medical technology.

- **SEC v. Kris Chellam** – SEC charged Kris Chellam, a former senior executive at a Silicon Valley technology company, for illegally tipping convicted hedge fund manager Raj Rajaratnam with nonpublic information that allowed the Galleon hedge funds to make nearly $1 million in illicit profits. Chellam was the 32nd defendant charged in the SEC’s Galleon-related enforcement actions.

- **SEC v. Robert D. Ramnarine** – SEC charged an executive at Bristol-Myers Squibb with insider trading on confidential information about companies being targeted for potential acquisitions.
Private Equity Enforcement Cases

• **Usurpation of investor opportunities:** In the Matthew Crisp action, an individual allegedly redirected an investment opportunity from private equity funds managed by Adams Street to a fund that he co-managed, the existence of which was not disclosed to Adams Street or its investors. In re Crisp, Adm. Proc. File No. 3-14520 *(instituted Aug. 30, 2012).*

• **Misallocation of expenses:** In the Robert Pinkas action, the principal of private equity manager Brantley Capital allegedly used funds from a private equity fund to pay for his defense in an unrelated SEC action. In re Pinkas, Adm. Proc. File No. 3-14759 *(instituted Feb. 15, 2012).*

• **Pyramid schemes:** In SEC v. Resources Planning Group, a private equity principal allegedly used fund assets to repay previous investors. No. 12-cv-9509 *(N.D. Ill. Filed Nov. 23, 2012).*

• **Insider trading:** In SEC v. Gowrish, a private equity firm employee allegedly stole confidential acquisition information and sold it for use in trading. No. 09-cv-5883 *(N.D. Cal. Filed Dec. 16, 2009).*

• **Value inflation:** In SEC v. Yorkville Advisors, a hedge fund allegedly inflated illiquid asset values. No. 12 Civ. 7728 *(S.D.N.Y. filed Oct. 17, 2012).*
How Will Dodd-Frank Weather the Coming Storm

Dodd-Frank & Law Practice

• Opportunities to develop a securities law practice
• Positions available in government
• Diversity and Inclusion Considerations, Rule 342
• Increased financial-regulation action; stepped-up enforcement and increased job opportunities?
Next Steps
Speaker Background

Kevin Armstrong  
General Counsel  
DST Brokerage Solutions, LLC

Kevin J. Armstrong is General Counsel of DST Brokerage Solutions, LLC (DSTBS). He serves on DSTBS’ Executive Management Committee and is responsible for all legal and regulatory activities of DSTBS and its affiliate, DST Market Services, LLC, a FINRA member broker-dealer and a SEC registered correspondent clearing firm. In this capacity, he interfaces with government and regulatory agencies on issues impacting the company.

Mr. Armstrong handles complex negotiations and oversees the legal risk management strategy to reduce and avoid regulatory risk and litigation while facilitating business growth and innovation.

Before joining DST Brokerage Solutions, LLC, Mr. Armstrong worked for Pershing Advisor Solutions LLC and its affiliated clearing broker dealer, Pershing LLC. Prior to joining, Pershing, Mr. Armstrong was a Vice President in the Legal and Compliance division at Morgan Stanley supporting growth for its Global Wealth Management and financial planning businesses.

Earlier in his career, Mr. Armstrong served as securities regulator in the Enforcement unit at FINRA (formerly the NASD). Prior to joining FINRA, Mr. Armstrong was a law clerk for the Honorable Lawrence M. Lawson, (Ret.) Assignment Judge, Superior Court of New Jersey. He is admitted to practice before the United States Supreme Court.

Mr. Armstrong is a former Chair of the Corporate Law Section of the National Bar Association (NBA); previously served as a member of the NBA’s Board of Governors. His memberships include the American Corporate Counsel Association and American Bar Association, Business Law Section. He serves on the Securities Industry Financial Markets Association’s (SIFMA) General Counsels Committee; and was recently appointed to the Lawyers’ Committee for Civil Rights Under Law Board of Trustees.

For his commitment to community service, in 2013, Mr. Armstrong received a CUP Catalyst: Change Agent award from the Council of Urban Professionals (CUP). The CUP award highlights and celebrates the accomplishments of individuals across the legal services sectors that have made an impact on their communities through business initiatives, board service, and mentorship and philanthropy efforts.

Mr. Armstrong is a frequent speaker on panels concerning broker-dealer law, diversity and inclusion initiatives in the legal profession and fundraising. He is an Honors graduate of Rutgers University where he received a B.S. degree in Management and he earned a J.D. degree from Rutgers School of Law–Newark.
Erica Y. Williams serves as Deputy Chief of Staff of the Securities and Exchange Commission where she advises on mission critical matters, regulatory policy and operational issues spanning all aspects of the Commission’s work. Ms. Williams became Deputy Chief of Staff in July 2012, and has served as counsel and adviser to three Chairs. In February 2011, she became counsel to Chair Mary L. Schapiro primarily focusing on enforcement matters. Ms. Williams joined the SEC in 2004 as Assistant Chief Litigation Counsel in the Enforcement Division’s trial unit, where she led trial teams in a number of successful prosecutions. In October 2009, Ms. Williams was named Federal Employee of the Week by Senator Ted Kaufman and was recognized on the floor of the U.S. Senate.

Prior to joining the SEC, Ms. Williams was a commercial litigator at a large law firm in Washington, D.C.

Ms. Williams received her bachelor’s degree and law degree from the University of Virginia.
In June 2010, Mr. Marchman joined the Financial Industry Regulatory Authority (FINRA) as Executive Vice President and Head of the Market Regulation Department’s Legal Group (the Group prosecutes violations of market rules and federal securities laws such as the recent significant disciplinary actions involving manipulative high-frequency trading activity).

Mr. Marchman, prior to joining FINRA, worked at New York Stock Exchange Regulation and during his tenure there headed the Market Surveillance Division, the Enforcement Division and the Regulatory Risk Group. While at NYSE Mr. Marchman directed several high profile and significant securities regulation disciplinary actions including the research analysts conflict of interest and specialist trading ahead cases.

Prior to joining the NYSE in 1989, Mr. Marchman was a Branch Chief in the U.S. Securities and Exchange Commission’s Division of Enforcement in Washington, D.C. While at the SEC Mr. Marchman brought a number of significant disciplinary actions including the action against Boyd Jefferies in connection with the Ivan Boesky insider trading case.

In addition to his securities regulation responsibilities, Mr. Marchman served as Chairman of NYSE Diversity Council from its inception in 1999 until his departure from the NYSE. At FINRA, Mr. Marchman serves on the company’s Executive Diversity Leadership Council (whose members include FINRA’s Chairman/CEO) as well as the Executive Sponsor of the FINRA’s Women’s Network Employee Resource Group.

Mr. Marchman is a magna cum laude graduate of Allegheny College, where he was inducted into Phi Beta Kappa and received his J.D. from the University of Pennsylvania. In addition, Mr. Marchman, the first African-American Executive Vice President at the NYSE, attended Harvard Business School’s Program for Management Development. Mr. Marchman’s involvement in civic affairs includes Board membership service as Operation HOPE (Chairman, Northeast Regional Board), PFLAG, The NSHSS Foundation, CEE, and the University of Pennsylvania Law School Board of Managers.
Rossie E. Turman III

Partner
Skadden, Arps, Slate, Meagher & Flom LLP
Banking

Rossie E. Turman III is a corporate attorney with a practice focus in leveraged finance, principally representing investment banks, commercial banks and other financial institutions as lenders; and corporations, strategic investors, hedge and BDC funds, and private equity funds as borrowers. Mr. Turman primarily advises clients in connection with syndicated loans, out-of-court and Chapter 11 reorganizations, acquisition financings, leveraged buyouts, bridge loans, asset-backed loans, subscription facilities, receivables facilities, project financings, and other types of complex and traditional transactions. Also, Mr. Turman is providing leadership in the firm’s efforts to expand its capacity to service clients engaged in cross-border transactions involving the African continent.

His work with corporate clients has included representations of Aflac, El Pollo Loco, Norfolk Southern Corp., The Providence Service Corporation and Spectra Energy. Institutional clients have included BlackRock, The Blackstone Group, Credit Suisse, ING and Wells Fargo. Additionally, Mr. Turman has been involved in a number of reorganizations and restructurings, including those of Kmart, Delphi and Spectrum Brands.

His work in Africa includes advising public and private entities, governments, parastatals, NGO’s and individual investors. He has been involved in transactions in the retail, infrastructure, energy, oil and gas, mining, agribusiness, technology and banking spaces. Mr. Turman also has actively supported several charities on the African continent for over two decades.

Mr. Turman has provided pro bono services for economic development activities, including representations for Abyssinian Development Corporation and the United Way in various transactions, and through his volunteer affiliations with Lawyers Alliance and the Community Law Office of Legal Aid. In 2013, he was named “Private Practitioner of the Year” by the Metropolitan Black Bar Association of New York City. Mr. Turman remains very active in training and mentoring associates in the firm and attorneys of color across the legal profession.
C. Annette Kelton is Managing Director and Associate General Counsel at Goldman Sachs & Co and in this role she heads the Equities Sales and Trading Coverage Group at Goldman Sachs, which guides the firm and its clients through the tricky terrain of regulatory and legal issues surrounding equities products and services.

Kelton earned a bachelor’s degree in business administration from Boston University and a law degree from Howard University School of Law. She went from federal clerk for the Hon. William F. Hall Jr. in the U.S. District Court for the Eastern District of Pennsylvania to serve as assistant district administrator in the Philadelphia District Office of the U.S. Securities and Exchange Commission before joining Goldman Sachs in 1999. Following her passion for finance law and having access to influential mentors like Hall and David J. Greenwald, Goldman Sachs’ deputy general counsel, helped to give her a successful career.

Kelton chairs the Buck County Chapter of the Links Inc. Youth Council, is a member of the Jersey Explorer Children’s Museum Board of Trustees, and educates youth about career opportunities in financial services through efforts such as Wall Street 101, a Jack and Jill of America Inc. annual event sponsored by Goldman Sachs.
Todd L. Cranford is the Director of Government Relations, Certified Financial Planner Board of Standards, Inc. (CFP Board) and in this newly created role, he works to advance the mission of CFP Board by advocating its public policy positions before Congress, the executive branch of the federal government, state legislatures and other state governmental offices.

Prior to joining CFP Board, Mr. Cranford was Of Counsel at Patton Boggs, LLP in Washington, D.C., where he developed and executed strategies to achieve clients' business and policy goals by engaging key policymakers. Before joining Patton Boggs in 2007, Cranford served as Senior Counsel on the Committee on Financial Services of the U.S. House of Representatives, advising former Chairman Barney Frank (D-Mass.) and members of the Committee on policy and legal issues related to capital markets and securities. He also held the position of Senior Counsel in the Division of Enforcement at the U.S. Securities and Exchange Commission, where he investigated, developed and instituted civil and administrative actions involving violations of federal securities laws.

Mr. Cranford’s other professional activities have included serving as Legislative Liaison in the Office of the Manhattan Borough President, National Advance Staff for the Clinton/Gore ’92 Campaign, Associate Attorney at Wilkie Farr & Gallagher in New York City, and Law Clerk for the Honorable Anna Diggs Taylor in Detroit, Mich.

Mr. Cranford earned his JD from the Columbia University School of Law in New York City and his BA from Dartmouth College in Hanover, N.H.
Appendix
In the Wake of Cyber Damage: Significant Decisions in Cybersecurity 2013–2014

By Roland L. Trope* and Lixian Loong Hantover**

I. INTRODUCTION

Cyber damage from intrusions into an enterprise’s information and operations networks will not surprise anyone but the ill-informed and those with their heads in the sand or in the “cloud.” What may be surprising is the coherence of legal decisions issued in the wake of cyber damage and the clarification of cyber responsibilities that clients and counsel will need to reckon with. To select decisions for discussion in this survey, we applied the following criteria. First, a court or regulator issued the decision between April 2013 and April 2014. Second, the decision assessed, or proposed standards for assessment of, an enterprise’s management of the cybersecurity of its data or operational systems. Third, the decision made a significant change to laws or regulations, or their interpretation. And, fourth, the decision deserves thoughtful consideration by counsel in light of its potential import for clients throughout the national economy. We review the selected decisions chronologically.

Part Two analyzes the Fifth Circuit decision in Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.,1 decided on September 3, 2013, involving bank claims of negligence against a payment processor for economic losses resulting from a data breach. Part Three analyzes the decision of the U.S. District Court for the District of New Jersey in FTC v. Wyndham Worldwide Corp.,2 filed on April 7, 2014, concerning, in part, a challenge to “the FTC’s authority to assert an unfairness claim in the data-security context.”3 Part Four examines the U.S. Department of Justice (“DoJ”) and Federal Trade Commission (“FTC”) Antitrust

* Roland L. Trope is a partner in the New York City offices of Trope and Schramm LLP and an Adjunct Professor in the Department of Law at the U.S. Military Academy at West Point. He can be contacted at rltrope@tropelaw.com.

** Lixian Loong Hantover is an associate in the Palo Alto offices of Wilson Sonsini Goodrich & Rosati. She can be contacted at lhantover@wsgr.com.

The views expressed by the authors are solely their own and should not be attributed to their respective law firms or to the U.S. Military Academy, the U.S. Department of Defense, or the U.S. government. The authors thank John D. Gregory, Candace Jones, Professor Sarah Jane Hughes, and Tom Smedinghoff for their insights and thoughtful contributions to this survey.

1. 729 F.3d 421 (5th Cir. 2013).
3. Id. at *2.
Policy Statement on Sharing of Cybersecurity Information, released on April 10, 2014, in which the DoJ and FTC explained why they do not believe that antitrust is, or should be, “a roadblock to legitimate cybersecurity information sharing” between private entities. Finally, Part Five assesses a cybersecurity initiative by the U.S. Securities and Exchange Commission’s Office of Compliance Inspections and Examinations (“OCIE”), which is “designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry’s recent experiences with certain types of cyber threats.”

II. LONE STAR NATIONAL BANK, N.A. v. HEARTLAND PAYMENT SYSTEMS, INC.

Do you assume that courts will deny recovery in tort for the economic costs flowing from data breaches? Don’t assume. Visa and MasterCard authorize certain “Issuer Banks” to issue payment cards (credit and debit cards). When a customer presents her credit card to a merchant, the merchant swipes the card to transmit confidential data of her account to an “Acquirer Bank,” which relays the data to a “Payment Processor,” that then forwards it to the Issuer Bank that issued the customer her card. The Issuer Bank checks if the cardholder has sufficient credit in her account and, if so, approves the payment and transmits its decision back through the chain (i.e., Issuer Bank to Payment Processor to Acquirer Bank to merchant). In this Visa and MasterCard network, there is a contract between a merchant and an Acquirer Bank, and a contract between an Acquirer Bank and a Payment Processor, but not between Issuer Banks and Payment Processors.

As early as December 2007, hackers obtained access to payment card information stored on the computer systems of a Payment Processor, Heartland Payment Systems, Inc. (“Heartland”). The hackers stole cardholder user names, passwords, credit and debit card numbers, and other personal identification information. Heartland did not discover the data breach until over a year later. By then, the hackers had exfiltrated millions of credit card numbers. Issuer

6. See Lone Star, 729 F.3d at 423.
7. Id.
8. Id.
9. See id.
10. Id. at 423, 426.
Banks whose customers were victims incurred costs to replace the compromised cards and to reimburse customers for fraudulent charges.\textsuperscript{15} Lacking a contract with Heartland, these Issuer Banks sued KeyBank (an Acquirer Bank) and Heartland\textsuperscript{16} alleging \textit{inter alia} that KeyBank “negligently failed to ensure that [Heartland’s] security procedures were sufficient to protect the financial data it received.”\textsuperscript{17} The district court dismissed the negligence action,\textsuperscript{18} holding it “inappropriate to create tort duties between sophisticated businesses that allocate risks through contract.”\textsuperscript{19} Faced with the uncertainty of whether the applicable law should be that of Texas, Ohio, or New Jersey, the court concluded that, in each of these jurisdictions, the economic loss doctrine\textsuperscript{20} would bar recovery in tort for the remediation costs incurred by Issuer Banks as the result of a data breach.\textsuperscript{21}

The Fifth Circuit reversed.\textsuperscript{22} It agreed with the Issuing Banks that, under New Jersey law, the economic loss doctrine did not preclude suits in tort to recover data-breach-related expenses even when there was no physical damage to the plaintiff.\textsuperscript{23} The Fifth Circuit relied on a New Jersey Supreme Court decision which held that damages caused by a defendant’s negligent conduct that interfered with a plaintiff’s business could be compensable in circumstances involving a \textit{foreseeable} and \textit{identifiable} class of plaintiffs.\textsuperscript{24}

The Fifth Circuit found the Issuer Banks constituted such an “identifiable class” because “Heartland had reason to foresee that Issuer Banks would be the entities to suffer economic losses were Heartland negligent, and because Heartland sends payment card information to the Issuer Banks, the “identities, nature, and number of victims are easily foreseeable.”\textsuperscript{25} The Fifth Circuit expressed concern that, without a tort remedy, the Issuer Banks appeared to have “no remedy for Heartland’s alleged negligence, defying ‘notions of fairness, common sense and morality.’”\textsuperscript{26}

\textsuperscript{15.} \textit{Heartland Payment Sys. Customer Data Sec. Breach Litig.}, 834 F. Supp. 2d at 575. Section 205.6 of Regulation E, in implementing the Electronic Fund Transfer Act, limits a consumer’s liability for unauthorized electronic fund transfers to $50, unless the consumer “fails to notify the financial institution within two business days after learning of the loss or theft . . . [in which case] the consumer’s liability shall not exceed . . . $500.” 12 C.F.R. § 205.6(b) (2014).

\textsuperscript{16.} \textit{Fin. Inst. Track Litig.}, 2011 U.S. Dist. LEXIS 34953, at *56. The Judicial Panel on Multidistrict Litigation consolidated lawsuits arising out of the data breach. Id. at *11.

\textsuperscript{17.} Id. at *74.

\textsuperscript{18.} Id. at *87.

\textsuperscript{19.} Id. at *82.

\textsuperscript{20.} Under the economic loss doctrine, a plaintiff seeking to recover purely economic losses, such as lost profits, generally is limited to contractual remedies. \textit{See} Lone Star Nat’l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 423 (5th Cir. 2013).

\textsuperscript{21.} \textit{Fin. Inst. Track Litig.}, 2011 U.S. Dist. LEXIS 34953, at *77–84.

\textsuperscript{22.} \textit{See} Lone Star Nat’l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 427 (5th Cir. 2013).

\textsuperscript{23.} Id. at 426.

\textsuperscript{24.} Id. (citing Carter Lincoln-Mercury, Inc., Leasing Div. v. EMAR Grp., Inc., 638 A.2d 1288, 1294 (N.J. 1994)).

\textsuperscript{25.} Id.

\textsuperscript{26.} Id. (quoting People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107, 116 (N.J. 1985)).
Although not a decision on the merits and limited to its interpretation of New Jersey law, *Lone Star Bank* reveals that judges in the Fifth Circuit are willing to allow recovery in tort for economic losses when the cause was negligently deficient cybersecurity practices of a third-party enterprise or by another party for which it was arguably responsible.27

### III. FTC v. Wyndham Worldwide Corp.

Did you doubt the FTC had the authority to take action for unfair practices in data security? The Wyndham case should give pause to those doubts. Wyndham Worldwide Corporation (“Wyndham”) controls the acts of hotel group subsidiaries.28 Under agreements with each subsidiary, Wyndham licenses the “Wyndham” name and requires each Wyndham-branded hotel to buy a specified computer system to handle reservations and payment card transactions (“Wyndham computer network”).29 Between April 2008 and January 2010, on three separate occasions, hackers gained unauthorized access to the Wyndham computer network and to customers’ payment card account numbers, security codes, and other stored data.30

The FTC brought an action against Wyndham under section 5(a) of the Federal Trade Commission Act, alleging Wyndham violated both prongs of section 5(a)’s prohibition of “acts or practices in or affecting commerce” that are ‘unfair’ or ‘deceptive’ by failing to provide reasonable and appropriate security for the personal information stored on the Wyndham computer network,31 and, after discovering the first two intrusions, for failing to “take appropriate steps in a reasonable timeframe to prevent the further compromise of such network.”32

Wyndham moved to dismiss on grounds that the FTC lacked authority to bring an unfairness claim regarding data security.33 The district court rejected what it viewed as Wyndham’s “invitation to carve out a data-security exception to the FTC’s unfairness authority.”34 Wyndham also contended that, even if the FTC had sufficient authority, its actions violated “basic principles of fair notice

---


29. Id. at *4.

30. Id. at *5–6.

31. Id. at *1 (quoting 15 U.S.C. § 45(a)(1)).

32. Id.

33. Id. at *6 (quoting Complaint for Injunction and Other Equitable Relief at 12, FTC v. Wyndham Worldwide Corp., No. 13-1887 (ES), 2014 U.S. Dist. LEXIS 47622, at *3–4 (D.N.J. Apr. 7, 2014)).

34. Id. at *11–12.

35. Id. at *16.
and due process” because the FTC had not issued guidelines to explain—and give fair notice of—what data-security practices would violate the “unfairness” standard.\(^{36}\) The court declined to find that fair notice could be achieved solely through the issuance of regulations,\(^{37}\) and observed that “the contour of an unfairness claim in the data-security context . . . is necessarily ‘flexible’ such that the FTC can apply section 5 ‘to the facts of particular cases arising out of unprecedented situations.’”\(^{38}\)

The court cautioned that it was not deciding liability and that its decision on the motion to dismiss “does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked.”\(^{39}\) However, it would be prudent for clients and counsel not to underestimate the FTC’s authority—or its willingness to use it—to protect consumers from unavoidable injury caused by a commercial enterprise’s deficient data-security practices.

IV. THE ANTITRUST POLICY STATEMENT ON SHARING OF CYBERSECURITY INFORMATION

Do you think information sharing of cyber threats will necessarily raise antitrust issues? The regulators think otherwise. In a letter dated June 2, 2000, the Electric Power Research Institute, Inc. (“EPRI”) asked the DoJ’s Antitrust Division to issue a “business review letter”\(^{40}\) regarding a proposed information exchange to “facilitate the energy industry’s ability to efficiently address” cyber threats and risks.\(^{41}\) The Antitrust Division responded favorably by letter, dated October 2, 2000, noting that The Report of the President’s Commission on Critical Infrastructure Protection (issued in 1997) had “concluded that intra-industry cooperation and information sharing is the quickest and most efficient way of protecting our critical infrastructure industries against cyber-threats.”\(^{42}\)

Nearly fourteen years later, on April 10, 2014, the DoJ and FTC (the “Agencies”) issued an Antitrust Policy Statement on Sharing of Cybersecurity Information

---

36. Id. at *27.
37. Id. at *38.
38. Id. at *40 (quoting FTC v. Colgate-Palmolive Co., 380 U.S. 374, 385 (1965)).
39. Id. at *11. In another case, the FTC was compelled to disclose the “data security standards” it intended to use to prove a party’s “data security was inadequate.” In re LabMD, Inc., No. 9357, slip op. at 1 (F.T.C. May 1, 2014) (order granting respondent’s motion to compel discovery), available at http://goo.gl/gZRAZT.
40. Under the business review procedure, the Antitrust Division of the DoJ may, in certain circumstances, review proposed business conduct and state its enforcement intentions. 28 C.F.R. § 50.6 (2013). Requesting parties accept an affirmative obligation to make full and true disclosure of the business conduct for which they request a review. See id. (Instruction 5).
(“Policy Statement”) in order to decrease uncertainty and allay concerns by private entities that information sharing between them about cyber threats might raise antitrust issues. The Policy Statement reiterates the DoJ’s 2000 analysis, namely that “properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns.”

In the Policy Statement, the Agencies acknowledge that the sharing of information between private entities about “incident or threat reports, indicators, threat signatures, and alerts (collectively, ‘cyber threat information’)” may improve the safety of the nation’s computer systems. The Policy Statement explains that, when the Agencies examine information sharing agreements, they will consider the “overall competitive effect of an agreement” and focus on whether, in light of its business purpose, such agreement “likely harms competition.” The Agencies make clear that certain practices within the private entities’ control will reduce the probability of competitive harm: avoiding disclosure of competitively sensitive information and of any conspiracy to make such disclosure; adopting safeguards to prevent or minimize such disclosure; and limiting the sharing of information to cyber threat information, such as threat signatures, source IP addresses, and target ports.

To date, the Antitrust Division has reviewed only one cybersecurity information sharing agreement—the one described in EPRI’s 2000 letter, which the Division approved. In light of this limited track record and the fact-intensive nature of such agreements and of any review by the Agencies, it would be prudent to study EPRI’s letter, the Division’s response, and the Policy Statement for guidance when structuring and implementing an agreement or mechanism for private entities to share cyber threat information.

V. THE OCIE’S CYBERSECURITY INITIATIVE

Do you think the SEC intends to “go easy” on cybersecurity? The OCIE’s latest initiative says otherwise. On April 15, 2014, the OCIE staff issued a National Exam Program Risk Alert (“Alert”) to explain its initiative to “assess cybersecurity preparedness in the securities industry and to collect data on the industry’s recent experiences with certain types of cyber threats.” The OCIE explains that it will examine “more than 50 registered broker-dealers and registered investment advisers regarding cybersecurity matters.”

---

44. Id. at 1.
45. Id. at 2–3 (footnotes omitted).
46. Id. at 5 (citation omitted).
47. Id. at 6.
48. Id.
49. Id. at 7.
51. Id.
In the Alert’s Appendix, the OCIE sets out the information it will request from each examined registered entity. The requested information appears aimed at enabling the OCIE to evaluate the extent to which a registered entity has formally and effectively created cybersecurity policies and practices to protect itself and its customers. For example, has the regulated entity made an organized and comprehensive assessment of the cyber threats to its operations and business from remote customer access and funds transfer requests from third parties that access its networks, customer data, and other sensitive information? What safeguards has the regulated entity implemented to detect unauthorized activity and to make measureable reductions in its exposure to such threats? What incidents has the regulated entity experienced? What losses were incurred or customer information accessed? What firm services were impacted? To what extent were these incidents reported to law enforcement, regulators, or industry organizations? It is worth noting that, although the Appendix represents that some of the questions track information outlined in the Framework for Improving Critical Infrastructure Cybersecurity, released on February 12, 2014 by the National Institute of Standards and Technology (“Framework”), the Appendix’s questions are more detailed, rigorous, and probing than those in the Framework. Regulators in other industries may also adopt initiatives that similarly exceed the minimum threshold set by the Framework. In that event, the Framework may fail to gain much traction. And, each critical infrastructure sector may continue building its own cybersecurity watchtower, setting its own safeguard standards, struggling to make correlations between cyber-threat information received from disparate sources, and focusing increasingly on the resilience needed to weather the worst case scenario: months or years of degraded infrastructure and slow recoveries from cyberattacks. Accordingly, boards of directors of registered entities and their counsel should make it a priority to consider enhancing their enterprise’s cybersecurity policies and procedures.

52. See id. at app., 1–7 (appending a sample list of requests for information that the OCIE may use when examining registered entities regarding cybersecurity matters).
53. Id. at 4.
54. Id.
55. Id. at 5–6.
56. Id. at 6–7.
57. Id.
VI. Conclusion

The coherence of the legal decisions reviewed in this survey stand in stark contrast to years of slow reaction to each bow wave of cyber damage to the nation’s economy. As of March 2013, the nation still lacked an “integrated strategic approach,”61 and as of April 2014, none has emerged. The adoption of digital technologies has come with what has proven to be a gross underestimation of the risk of cyberattacks, the undiminished vulnerability to such attacks, and the growing extent of damage they can inflict. The decisions we have discussed will not reverse those trends. Instead, they incrementally adjust who bears the burdens of the continued deferral of a coherent federal response to cyberattacks. They illustrate that liability from inattention appears to be an emerging risk and may become the impetus that enterprises need to justify investment in enhanced cybersecurity practices. And they should help reduce impediments the private sector must overcome as it jury-rigs responses to belated discoveries of successful attacks.