MAYER·BROWN

Board's Risk Oversight Function

January 2016

Edward S. Best
Partner
312.701.7100
ebest@mayerbrown.com

- Sources of Duty
- Types of Risk
- Who Should Fulfill the Oversight Responsibility
- Elements of Effective Risk Management Oversight

Sources of Duty

- Delaware Fiduciary Law
  - A board's risk oversight responsibility derives primarily from state law fiduciary duties
    - To be clear, the board cannot and should not be involved in actual day-to-day risk management. Its role is limited to oversight.
  - Generally, directors can only be liable for a failure of board oversight where there is "sustained or systemic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists." *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959, 971 (Del. Ch. 1996).
  - In cases since Caremark, the Delaware courts have made clear that there would be no liability under a *Caremark* theory unless the directors intentionally failed entirely to implement any reporting or information system or controls or, having implemented such a system, intentionally refused to monitor the system or act on warnings it provided.

Sources of Duty

- New York Stock Exchange Rules
  - NYSE rules impose certain risk oversight obligations on the audit committee of a listed company, while acknowledging that "it is the job of the CEO and senior management to assess and manage the listed company's exposure to risk"
  - NYSE rules require that an audit committee "discuss guidelines and policies to govern the process by which risk assessment and management is undertaken."
  - Discussions should address major financial risk exposures and the steps the company has taken to monitor and control such exposure, including a general review of the company's risk management programs
  - NYSE rules permit a company to create a separate committee or subcommittee to be charged with the primary risk oversight function as long as the risk oversight processes conducted by that separate committee or subcommittee are reviewed in a general manner by the audit committee, and the audit committee continues to discuss policies with respect to risk assessment and management

Sources of Duty

- Other Sources
  - SEC
    - Proxy statements must disclose any compensation policies or practices that create risks that "are reasonably likely to have a material adverse effect on the company"
    - Proxy statements must disclose the extent of the board's role in risk oversight, including a description of how the board administers its oversight function
  - "Best Practices"
    - National Association of Corporate Directors—Blue Ribbon Commission on Risk Governance
    - Committee of Sponsoring Organizations of the Treadway Commission
    - Conference Board Corporate Governance Center
  - Institutional Shareholder Services
    - Includes a specific reference to risk oversight as a criteria for choosing to recommend or oppose a director for election

Sources of Duty

- Other Sources
  - Industry specific laws, rules and guidelines
    - Insurance Companies
      - NAIC Corporate Governance Annual Disclosure Model Act requires insurers to describe corporate governance, including "The processes by which the Board of Directors, its committees and senior management ensure an appropriate level of oversight to the critical risk areas impacting the insurer's business activities including risk management processes, the actuarial function, and investment, reinsurance and business strategy decision-making processes."
    - Banks
      - Federal Reserve Board rules adopted under Dodd-Frank require all covered companies, as well as publicly-traded bank holding companies with $10 billion or more in assets, to create a risk committee to oversee risk management practices on an enterprise-wide basis. The committee must have at least one independent director and at least one member with relevant risk management expertise. Each member of the committee must have an understanding of relevant risk management principles and practices.

Types of Risk

- Financial Reporting Risk and Fraud
- Credit Risk
- Liquidity Risk
- Operational Risk
- Investment Risk
- Privacy and Cyber Security Risk
- Environmental Risk
- Legal/Compliance Risk
- Tax Risk
- Reputational Risk

Who Should Fulfill the Oversight Responsibility

- Some commentators believe that risk oversight is equal in importance to oversight of strategy and that the full board should have responsibility
  - Delaware law imposes the duty of oversight on all directors
- NYSE rules require the audit committee to address major financial risk exposures
- Some commentators believe the audit committee is already overburdened and that a separate risk committee is appropriate
- Some commentators would "split the baby" and have the audit committee oversee financial/accounting risks and the full board or another committee other risks
- ONE SIZE DOES NOT FIT ALL

Elements of Effective Risk Management Oversight

- Identification
  - Identify categories of risk the company faces, including concentrations and interrelationships
  - Identify potential actors that pose risk and stakeholders who are subject to risk
  - Review assumptions and analysis underpinning the determination of the company's principal risks
  - Ensure procedures are in place to identify new or materially changed risks
- Measurement
  - Understand the likelihood of occurrence (frequency) and the potential impact (severity) of risks
  - Review the ways in which risk is measured on an aggregate, company-wide basis

Elements of Effective Risk Management Oversight

- Limits
  - Understand how aggregate and individual risk limits (quantitative and qualitative, as appropriate) are set
  - Review actions to be taken if risk limits are exceeded
- Mitigation
  - Review risk mitigation measures
  - Review response plans
- Responsibility
  - Set the correct "tone at the top"
  - Allocate responsibilities for risk oversight and management of specific risks to ensure a shared understanding as to accountabilities and roles
  - Consider cross-disciplinary teams where appropriate

Elements of Effective Risk Management Oversight

- Communication
  - Review procedures for reporting matters to the board
  - Review quality, type and format of risk-related information provided to board
  - Review how risk management strategy is communicated and integrated into the enterprise-wide business strategy
- Assessment
  - Review the design of the company's risk management functions, as well as the qualifications and backgrounds of senior risk officers
  - Assess whether management is following risk policies and procedures
  - Confirm internal audit includes assessment of risk management
- Compensation
  - Review the company's compensation structure to ensure it is creating proper incentives in light of risks

Presentation at The Directors Roundtable

Mayer Brown Conference Center, 1221 Ave. of the Americas
New York, NY

January 6, 2016

8:30 a.m. – 10:45 a.m.

HEISENBERG'S UNCERTAINTY PRINCIPLE, EXTRATERRITORIALITY AND COMITY

John DeQ Briggs & Daniel S. Bitton***
Axinn Veltrop & Harkrider LLP
Washington, D.C. & New York, NY

I. INTRODUCTION[1]

The American legal system is different from any other legal system in the world. One consequence of that reality is that

* Mr. Briggs is Co-chair of the Antitrust & Competition practice at Axinn Veltrop & Harkrider LLP, Managing Partner of the firm's Washington, DC, office, and a former Chair of the Section of Antitrust Law of the American Bar Association. He is also an Adjunct professor of International Competition Law at the George Washington Law School as well as a long-time member of various advisory boards for Competition publications.

** Mr. Bitton is a partner in the Antitrust & Competition practice at Axinn Veltrop & Harkrider LLP. His practice is focused on counseling and representing clients in high-stakes international antitrust matters, including global merger clearance, government non-merger investigations, and litigation. Before he moved from The Netherlands to the U.S. and joined Axinn in 2004, he was a legal advisor to the Netherlands Competition and Post and Telecommunications Authorities (before their operations were merged into one agency in 2013).

1. This is a companion piece to Mr. Briggs' earlier article, *Schrödinger's Cat and Extraterritoriality*, 29 ANTITRUST MAGAZINE 79 (Fall 2014). The German physicist, Werner Heisenberg was a contemporary of Schrödinger. Introduced first in 1927, the principle states that the more precisely the position of some particle is determined, the less precisely its momentum can be known, and vice versa. It is related to a similar effect in physics called the "observer effect," which notes that measurements of certain systems cannot be made without affecting the systems being observed. *See Uncertainty principle*, WIKIPEDIA, https://en.wikipedia.org/wiki/Uncertainty_principle.

In the context of this article, the reference to Heisenberg is mainly intended to take note of the reality that whether, when, and under what circumstances

much of the rest of the world is locked into a love/hate relationship with our legal system. On the "love" side, foreign individuals and enterprises regularly seek access to the American legal system because of the perception, and sometimes the reality, that it provides generous benefits to persistent plaintiffs who can find a wrongdoer defendant over whom a U.S. court can claim jurisdiction. On the "hate" side, foreign businesses, as well as foreign governments, increasingly seem to resent the lack of respect that American courts give to the views and interests of foreign sovereigns, enterprises, and citizens.

Across the legal landscape, American courts assert jurisdiction over foreign enterprises and individuals for conduct occurring outside the United States in both criminal and civil cases. While the issues in criminal cases are significant, and sometimes the cause of quiet foreign sovereign annoyance, it is the civil cases that seem to create the greatest tensions, at least publicly. The civil cases most usually arise in settings where private plaintiffs are making claims that involve multiple damages and attorney's fees, such as antitrust and Racketeer Influenced Corrupt Organizations (RICO) cases, or other cases where damage claims are large (i.e., securities claims) or where there exist clear opportunities for substantial punitive damages of the sort rarely available in the courts of other countries (i.e., tort claims). Private civil claimants and their counsel in these types of cases have every incentive to persuade American courts to take jurisdiction over foreign defendants and foreign conduct. Indeed, attorneys have an ethical duty to advance their clients' claims as vigorously as possible, which more or less requires them to

---

American courts will assert extraterritorial jurisdiction over foreign conduct by foreign actors, and whether, when, and under what circumstances those same courts will consider or apply any principles of comity is regrettably uncertain and has much to do with the presence or absence of such occasional judicial oversight as might from time to time be present.

push domestic courts to the limits of their jurisdiction, if not beyond.

For its part, the government, especially in recent years, has advanced relatively expansive theories of the extraterritorial reach of U.S. laws.[2] In antitrust cases, the statistics are staggering. The Antitrust Division of the Department of Justice (DOJ) has long been proud of its sentencing of individuals to jail for their antitrust infringements, without really highlighting the reality that many individuals sentenced are foreigners.[3] That same Antitrust Division seems to be even prouder of the many billions of dollars in fines that it has collected annually for the last

---

2. *See, e.g.*, Brief for the United States and the Fed. Trade Comm'n as Amici Curiae in Support of Neither Party on Rehearing En Banc at 8, Minn-Chem, Inc. v. Agrium Inc., 683 F.3d 845, 856-57 (7th Cir. 2012) (No. 10-1712), 2012 WL 6641190 (urging the Seventh Circuit to hold, as it did, that the word "direct" in the Foreign Trade Antitrust Improvements Act (FTAIA) should be interpreted to mean only a "reasonably proximate" causal nexus); *but see* Brief for the United States as Amicus Curiae Supporting Reversal, Sachs v. Republic of Austria, 737 F.3d 584 (9th Cir. 2013), *cert. granted sub nom*. OBB Personenverkehr AG v. Sachs, 135 S. Ct. 1172, 190 L. Ed. 2d 929 (2015) (urging that a foreign state may be held to carry on commercial activity in the United States through the application of common-law agency principles, but criticizing the Ninth Circuit's view that the buying of a ticket for an Austrian train amounted to an element of the plaintiff's strict liability claim. The fact that the Supreme Court has agreed to hear the case suggests that the Court might well be concerned about the inclination of various courts to engage in the extraterritorial application of American legal principles, in this case a tort principle of strict liability).

3. The most recent DOJ Antitrust Division statistics reflect that for the five-year period 2010-14: criminal fines collected amounted to nearly $4 billion; almost 400 defendants were charged with criminal antitrust offenses and more than 300 actual cases were filed; the average prison sentence was 25 months. *See Sherman Act Violations Yielding a Corporate Fine of $10 Million or More*, U.S. DEP'T OF JUSTICE (July 7, 2015), http://www.justice.gov/atr/sherman-act-violations-yielding-corporate-fine-10-million-or-more; *see also Criminal Enforcement Fine and Jail Charts*, U.S. DEP'T OF JUSTICE (June 25, 2015), http://www.justice.gov/atr/criminal-enforcement-fine-and-jail-charts.

several years from antitrust cartelists, although it does not quite so heavily advertise the reality that the overwhelming majority of these fines are collected from foreign companies for conduct that took place in foreign lands.[4]

The Antitrust Division data show that of the 124 companies suffering fines in excess of $10 million, 110 were foreign. Of those, 67 were Asian, 38 European, and only 14 American.[5] Nearly without exception, these criminal "prosecutions" are the product of guilty pleas brought about by and large as a result of the American, European, or other leniency programs.[6] Indeed, in recent years, it is rare that a case goes to trial and results in a sentencing process that involves a district court rendering a decision to which the prosecution and defendant have not already agreed.[7]

Judges, especially federal judges with life tenure, seem to have very little incentive to exercise restraint in the exercise of their own extraterritorial jurisdiction. In antitrust, for example, where foreign non-import conduct generally is only possibly actionable if it produced a "direct, substantial, and reasonably foreseeable effect" in the United States,[8] many U.S. courts (at the urging of the DOJ and private plaintiffs) increasingly have viewed those words as expansive, and decreasingly have

---

4. *Criminal Enforcement Fine and Jail Charts*, *supra* note 3.

5. *Sherman Act Violations Yielding a Corporate Fine of $10 Million or More*, *supra* note 3.

6. *See* Scott D. Hammond, *The Evolution of Criminal Antitrust Enforcement over the Last Two Decades*, presented at the Nat'l Institute on White Collar Crime, U.S. DEP'T OF JUSTICE at 3, 8 (2010) (discussing the success of leniency programs in the United States and efforts to implement similar programs by foreign countries).

7. *United States v. Hui Hsiung*, 778 F.3d 738 (2014), *cert. denied*, 2015 WL 1206283, is a rare example of this type of case.

8. 15 U.S.C. § 6a (2012).

viewed them as words of restraint.[9] Even the Supreme Court initially seemed to use these words to eliminate much of a role for comity,[10] but more recently reversed course on that.[11]

And while the Supreme Court increasingly has urged lower courts to exercise restraint in the extraterritorial application of U.S. law,[12] and has urged lower courts to take into account principles of comity,[13] those exhortations strangely seem not to have taken much root in the lower courts. In other words, the American courts are operating in the area of extraterritorial

---

9. *See, e.g.*, Minn-Chem, Inc. v. Agrium Inc., 683 F.3d 845, 857 (7th Cir. 2012) (interpreting the word "direct" as "reasonably proximate" rather than the more limited "immediate").

10. *See* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 798 (1993) (stating international comity considerations would arise only if there were a "true conflict between domestic and foreign law"). In his dissent, Justice Scalia invoked a canon of statutory construction to the effect that an act of Congress should not be construed as violating international law if any other possible interpretation is available. *Id*. at 814-15.

11. F. Hoffman-La Roche Ltd. v. Empagran S.A., 542 U.S. 155, 164-69 (2004) (following Scalia's logic in his *Hartford Fire* dissent by invoking international comity considerations in denying extraterritorial application of U.S. antitrust laws, even though the conduct at issue was unlawful under foreign law as well, because "American private treble-damages remedies to anticompetitive conduct taking place abroad had generated considerable controversy.").

12. *See, e.g.*, M/S Bremen v. Zapata Off-Shore Co., 407 U.S. 1, 9 (1972) (stating "[w]e cannot have trade and commerce in world markets and international waters exclusively on our terms, governed by our laws, and resolved in our courts."); Morrison v. National Australia Bank Ltd., 561 U.S. 247 (2010) (It is a "longstanding principle of American law that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.") (internal citations and quotations omitted).

13. *See, e.g.*, Daimler AG v. Bauman, 134 S. Ct. 746, 763 (2014) (chastising the lower court for insufficiently considering international comity); *Empagran*, 542 U.S. at 164-65.

jurisdiction without close or regular supervision, and with few objective or clear restraining guidelines that provide limiting principles.

The Supreme Court has held that "where issues arise as to jurisdiction or venue, discovery is available to ascertain the facts bearing on such issues."[14] So, even when jurisdiction is contested, district court judges exercise considerable discretion to authorize "jurisdictional discovery," so that the court can determine its jurisdiction. This jurisdictional discovery is regularly conducted under the auspices of Rule 26 of the Federal Rules of Civil Procedure, which normally authorizes the broadest imaginable discovery. And so a rule authorizing nearly unlimited discovery is called into play to authorize plaintiffs to rummage through foreign files of foreign companies and foreign persons to develop evidence that might persuade an American court that it, in fact, has jurisdiction over the foreign enterprise, or over a domestic enterprise, for foreign conduct with some perceptible impact on American commerce. There is, however, no consensus regarding the circumstances in which jurisdictional discovery should or will be granted and the circuits are by no means uniform on this subject.[15]

Few if any other legal systems in the world involve circumstances where powerful courts are called upon by private parties to exercise extraterritorial jurisdiction over foreign companies, individuals, and conduct. For many people, including even relatively sophisticated judges, lawyers, and academics, this proposition is seen as unremarkable. The bench and the bar in this country seem to accept the fact of this extraordinary

14. Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351 n.13 (1978) (citing MOORE'S FEDERAL PRACTICE ¶ 26.56[6] (2d ed. 1976)).

15. For an especially trenchant and thorough discussion of this entire issue, *see* S. I. Strong, *Jurisdictional Discovery in United States Federal Courts*, 67 WASHINGTON & LEE L. REV. 489 (2010).

power as if it were an obvious adjunct to "American Exceptionalism."[16] But in nearly all other countries, the exercise of extraterritorial jurisdiction is more rare, and nearly always at the behest of a government acting through its executive branch or its legislature. Foreign courts seem to show more restraint in the exercise of their power, which is in any case more limited than that enjoyed by American courts. This might be changing. As the People's Republic of China (PRC), along with other powerful countries, observe the American legal system, "learn" from it, and mimic it to their advantage, American or other firms whose conduct outside China can be claimed to have some perceptible effect on Chinese commerce will come to be treated in much the same way that our system treats Asian and European companies. Indeed this is already happening.[17]

It is the purpose of this article to begin to explore this area and to try to come up with a workable understanding of what comity means or should mean or might mean and, in the end, to

---

16. There is also the related matter of the extraordinary power of American courts in general and the underlying reasons for that. As Francis Fukuyama observes: "The story of the [American] courts is one of the steadily increasing judicialization of functions that in other developed democracies are handled by administrative bureaucracies, leading to an explosion of costly litigation, slowness of decision-making, and highly inconsistent enforcement of laws. In the United States today, instead of being constraints on government, courts have become alternative instruments for the expansion of government." Francis Fukuyama, *America in Decay: The Sources of Political Dysfunction*, 93 FOREIGN AFFAIRS, Sept.-Oct. 2014, at 5, 11.

17. *See, e.g.*, Michael Martina & Mathew Miller, *As Qualcomm Decision Looms, U.S. Presses China on Antitrust Policy*, REUTERS (Dec. 16, 2014), http://www.reuters.com/article/2014/12/16/qualcomm-china-antitrust-idUSL3N0TW2SF20141216 (noting that President Obama admonished "China against applying its anti-monopoly law to benefit Chinese firms using foreign companies' technology," and that, moreover, "[a]t least 30 foreign firms . . . have come under the scrutiny of China's 2008 anti-monopoly law, which some critics say is being used to unfairly target non-Chinese companies.").

propose some possible courses of action that might bring to this issue the attention we believe it deserves, to rein in somewhat the largely uncabined extraterritorial jurisdiction of American courts, and to bring the exercise of judicial extraterritoriality more into line within international norms.

II. RUFFLED FEATHERS: MANY FOREIGN GOVERNMENTS TAKE ISSUE WITH AMERICAN "LEGAL IMPERIALISM"

In a variety of settings foreign governments have expressed and are expressing concerns about the extraterritorial application of U.S. law. The United States occupies a unique position in global trade and finance. The United States also has enacted far-reaching legislation involving commerce, banking and finance, business conduct, mergers and acquisitions, foreign corrupt practices, and a variety of other matters. The extraterritorial application of laws in these areas challenges the sovereignty of other nations and is often viewed as offensive. In antitrust, the United States' influence is the result of its status as the world's largest importer of goods and services.[18] In finance, this influence is the result of the U.S. dollar's status as the international unit of account: "Pretty much any dollar transaction—even between two non-US entities—will go through New York

18. *Int'l Trade Statistics*, WORLD TRADE ORG. 26, 28 (2014), https://www.wto.org/english/res_e/statis_e/its2014_e/its2014_e.pdf; *cf.* Brief for the Government of Canada as Amicus Curiae Supporting Reversal, at 1, F. Hoffmann-La Roche, Ltd. v. Empagran S.A., 542 U.S. 155 (2004) (No. 03-724), 2004 WL 226389 (noting that the effect of U.S. laws on Canadian policy is heightened by the level of "interdependence of the economies of Canada and the United States, which enjoy the largest bilateral trading relationship in the world[.]") [hereinafter Canada Empagran Amicus].

City at some point, where it comes under the jurisdiction of US authorities."[19]

The rampant extraterritorial application of U.S. laws has ruffled the feathers of foreign governments for a long time, beginning essentially with the cluster of private and government actions in the Uranium cartel cases back in the 1970's and 1980's. Close American allies, including Australia, Canada, France, South Africa, the UK, and others, reacted with hostility to the extraterritorial activism of the domestic judiciary by enacting "blocking" and "claw back" legislation.[20] Such reactions included the enactment of laws by the United Kingdom and Canada that prohibit enforcement of foreign judgments awarding multiple damages[21] and laws passed by the United Kingdom, France, Australia, and the Canadian provinces of Quebec and Ontario that limit or prohibit the removal of documents in response to a foreign order.[22]

---

19. Felix Salmon, *America prosecutes its interests and persecutes BNP*, FIN. TIMES (June 5, 2014), http://www.ft.com/intl/cms/s/0/edbec3b0-eca3-11e3-8963-00144feabdc0.html.

20. *See* Briggs, *supra* note 1, at 79.

21. *See* UK and Netherlands Empagran Amici, *infra* note 23, at 17-18 ("The private actions . . . caused several countries, including the United Kingdom, to enact statutes blocking discovery of documents and other information needed to prosecute foreign defendants[,] . . . restrict[ing] enforcement of treble damage judgments and allow[ing] both firms and persons conducting business in the United Kingdom to sue in the UK to 'claw back' the penal portion of the foreign judgment . . . ."); Germany and Belgium Empagran Amici, *infra* note 23, at 27 n.11 (citing examples of United Kingdom and Canadian "blocking" and "claw back" laws).

22. *See* UK and Netherlands Empagran Amici, *infra* note 23, at 17 (citing the United Kingdom as one example of a country that passed a law making document discovery more difficult as a result of private actions in the United States); Germany and Belgium Empagran Amici, *infra* note 23, at 27

More recently, a number of governments have expressed their concerns about the application of U.S. laws abroad through amicus briefs, including Australia, Belgium, Canada, China, France, Germany, Japan, the Netherlands, South Korea, Switzerland, Taiwan, and the United Kingdom:[23] most of the United States' top fifteen trading partners.

(discussing United Kingdom, French, Australian, and Canadian laws prohibiting removal of domestic corporation documents pursuant to a foreign court order).

23. *See, e.g.*, Brief of the Government of the Commonwealth of Australia as Amicus Curiae in Support of the Defendants-Appellees, Morrison v. Nat'l Australia Bank Ltd., 130 S. Ct. 2869 (2010) (No. 08-1191), 2010 WL 723006 [hereinafter Australia Morrison Amicus]; Brief of the Governments of the Federal Republic of Germany and Belgium as Amici Curiae in Support of Petitioners, F. Hoffmann-La Roche, Ltd. v. Empagran S.A., 124 S. Ct. 2359 (2004) (No. 03-724), 2004 WL 226388 [hereinafter Germany and Belgium Empagran Amici]; Canada Empagran Amicus, *supra* note 18; Brief of the Ministry of Commerce of the People's Republic of China as Amicus Curiae in support of the Defendants' Motion to Dismiss, *In re* Vitamin C Antitrust Litig., 810 F.Supp.2d 522 (E.D.N.Y. 2011) (No. 06-md-01738), 2006 WL 6672257 [hereinafter China Vitamin C amicus]; Brief for the Republic of France as Amicus Curiae in Support of Respondents, Morrison v. Nat'l Australia Bank Ltd., 130 S. Ct. 2869 (2010) (No. 08-1191), 2010 WL 723010 [hereinafter France Morrison Amicus]; Brief of the Government of Japan as Amicus Curiae in Support of Petitioners, F. Hoffmann-La Roche, Ltd. v. Empagran S.A., 124 S. Ct. 2359 (2004) (No. 03-724), 2004 WL 226390 [hereinafter Japan Motorola Amicus]; Brief of the United Kingdom of Great Britain and Northern Ireland, Ireland and the Kingdom of the Netherlands as Amici Curiae in Support of Petitioners, F. Hoffmann-La Roche, Ltd. v. Empagran S.A., 124 S. Ct. 2359 (2004) (No. 03-724), 2004 WL 226597 [hereinafter UK and Netherlands Empagran Amici]; Brief of the Korea Fair Trade Commission as Amicus Curiae in Support of Appellees' Opposition to Rehearing En Banc, Motorola Mobility LLC v. AU Optronics Corp., 775 F.3d 816 (7th Cir. 2015) (No. 14-8003), 2014 WL 2583475 [hereinafter Korea Motorola Amicus]; Letter of Ministry of Economic Affairs, Republic of China, Taiwan as Amicus Curiae to Express Its Views Regarding Application of the Foreign Trade Antitrust Improvement Act, Motorola Mobility LLC v. AU Optronics Corp., 775 F.3d 816 (7th Cir. 2015) (No. 14-8003). The European Commission also filed an amicus brief

These foreign governments have expressed a fairly wide variety of concerns about the potential for extraterritorial application of U.S. laws to interfere with those governments' policy decisions on such matters as liability, procedure, and damages. While most governments have regulatory regimes in place to police, for example, securities fraud and cartel behavior, these differ in many regards both from the American approach and also from each other, reflecting different cultural, social, and economic factors. These differences include the required showing for liability (e.g., definition of materiality in securities fraud cases),[24] procedural protections (e.g., class-action formation and

in *Kiobel*. Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party, Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659 (2013) (No. 10-1491), 2012 WL 2165345.

24. *See* Brief of the United Kingdom of Great Britain and Northern Ireland as Amicus Curiae in Support of Respondents at 16-17, Morrison v. Nat'l Australia Bank Ltd., 130 S. Ct. 2869 (2010) (No. 08-1191), 2010 WL 723009 (noting that U.K. securities laws differ from U.S. laws in their respective definitions of "materiality" and in their imposed obligations to disclose, which "are not only matters of language or nuance; they reflect legitimate policy decisions") [hereinafter UK Morrison Amicus]; France Morrison Amicus, *supra* note 23, at *23 (stating countries "often have different schemes of disclosure, different pleading and substantive standards for scienter, different standards of reliance, materiality and causation, different rules governing contribution and indemnity, and different limitations periods.") (footnote omitted).

cost-shifting provisions),[25] and the availability of multiple (i.e., punitive) damages.[26] Applying U.S. law to actors, conduct, and effects appropriately considered under a set of foreign laws undermines a foreign government's ability to govern its own domain and, in the end, becomes an affront to its sovereignty.

Stepping on the toes of foreign governments' regulatory regimes also risks stymying the international development of policies and regulations beneficial to the United States. Countries without well-developed regulatory apparatuses are less

25. *See* UK Morrison Amicus, *supra* note 24, at *19 (noting that U.K. law conflicts with U.S. procedural rules for: "(i) The scope of discovery; (ii) The availability of class actions or other forms of multi-party litigation; (iii) The availability of 'opt-out' classes, whether by default or in the court's discretion; (iv) The availability of contingency fee arrangements for plaintiffs' counsel; (v) The availability of attorney's fee awards against an unsuccessful party; (vi) The legality of third-party litigation funding; (vii) The availability of jury trials; and (viii) The expected time to bring a case to trial"); France Morrison Amicus, *supra* note 23, at *24 ("Foreign jurisdictions also generally have different rules governing attorney's fees, contingency fees, jury trials, and pretrial discovery. Although those rules are often characterized as 'procedural,' they have substantial practical effect and application of U.S. rules to foreign securities transactions could upset a foreign nation's carefully thought out balancing of plaintiffs' and defendants' interests.") (footnote omitted).

26. *See* Japan Motorola Amicus, *supra* note 23, at 5 ("The Japanese law and the laws of many (if not all) countries other than the US do not provide for treble damage awards in antitrust claims. Treble damages would be viewed as punitive damages, mixing civil and criminal liability."); Korea Motorola Amicus, *supra* note 23, at 3-4 (noting that Korea's antitrust laws do not provide multiple nor punitive damages); France Morrison Amicus, *supra* note 23, at *23 (noting that "many foreign nations do not permit the award of punitive damages"); Australia Morrison Amicus, *supra* note 23, at 22 (same).

likely to develop them if the behavior is already policed by private plaintiffs in the United States or if the apparatuses would see their policy choices effectively overruled by U.S. policies.[27]

Foreign governments have also taken the view that extraterritorial application of treble damages threatens to undermine their own enforcement efforts. For example, they claim availability of private treble damages in the United States against their national companies for local conduct may have a detrimental effect on foreign leniency programs. These programs are a key tool for them in rooting out cartel activity, which has traditionally proven difficult to detect and prosecute.[28] "These leniency policies seek to balance the interests of disclosure, deterrence, and punishment," but "disclosure and reform are greatly hindered when a company risks the imposition of treble damages in a U.S. court for confessing to another nation or authority that

27. *See* Canada Empagran Amicus, *supra* note 18, at 20-21 (arguing that applying U.S. law too broadly would "remove the incentives of other foreign jurisdictions to implement comprehensive antitrust enforcement regimes and to expand their cooperative efforts . . . Thus, the unilateral assertion of jurisdiction by the United States would, ultimately, impair the interests of the United States in effective mutual cooperation and enforcement."); *cf.* China Vitamin C Amicus, *supra* note 23, at 6 (arguing that application of U.S. antitrust policies to Chinese "regime instituted to ensure orderly markets" would harm China's "transition to a market-driven economy").

28. *See* Korea Motorola Amicus, *supra* note 23, at 4 ("Like the U.S. Department of Justice and the European Commission, the KFTC has adopted a delicately balanced leniency program that effectively detects and deters cartel activities, which by nature are often undertaken in secret."); Brief of the Belgian Competition Authority as Amicus Curiae in Support of Appellees' Position Seeking Affirmation of the District Court's Order at 8, Motorola Mobility LLC v. AU Optronics Corp., 775 F.3d 816 (7th Cir. 2015) (No. 14-8003), 2014 WL 5422010 (noting that the Belgium competition authority "relies to a significant extent on that leniency program to enforce unlawful restraints of trade.").

it has participated in an international conspiracy."[29] When that reach is expanded outside of U.S. consumers in a U.S. court, "the prospect of ruinous civil liability in U.S. courts far outweighs the benefits most companies would receive from participating in an amnesty program."[30] And as Germany and Belgium informed the Supreme Court in *Empagran*,[31] "[h]istorically, other nations have bristled at extraterritorial applications of United States antitrust laws. These concerns have resulted in foreign governments taking a number of measures to counter what they perceive to be an illegitimate encroachment into their sovereignty."[32]

The enforcement of American law against foreign enterprises for their foreign conduct has become increasingly contentious and offensive, especially quite recently. The displeasure of the PRC seems particularly acute. In the *Vitamin C* litigation, a substantial treble damage jury verdict was entered against companies chartered by the PRC for their involvement in an export price-fixing cartel that the PRC itself claimed was conduct directed by a foreign sovereign in order to assure compliance with U.S. antidumping laws. The District Court rejected the interpretation of Chinese law advanced by the PRC and held that, under Rule 44.1 of the Federal Rules of Civil Procedure, the construction of foreign law was a factual matter for the court itself and that only "some degree of deference" was owed to the foreign

29. Germany and Belgium Empagran Amici, *supra* note 23, at *29-30.

30. *Id.* at *30; *see also* Korea Motorola Amicus, *supra* note 23, at 4 ("[F]iling for leniency with non-U.S. antitrust authorities might actually result in a greater likelihood of facing private antitrust damages actions in the United States.").

31. F. Hoffmann-La Roche, Ltd. v. Empagran S.A., 542 U.S. 155 (2004).

32. Germany and Belgium Empagran Amici, *supra* note 23, at *25.

sovereign's statement as to the meaning of its own law.[33] The case is now on appeal to the Second Circuit, where the PRC, through its Ministry of Foreign Commerce (MOFCOM), has filed a strong amicus brief expressing the view that the district court's dismissive attitude towards the foreign sovereign's explanation of its own law was "profoundly disrespectful and wholly unfounded." The brief further stated that "the district court's approach and result have deeply troubled the Chinese government, which has sent a diplomatic note concerning this case to the U.S. State Department."[34]

It is not just foreign governments who react angrily to what some call American Judicial Imperialism. Consider the reaction outside of the United States to a statute that took effect on July 1 of last year—the Foreign Account Tax Compliance Act (FATCA). It is not well known that the United States is virtually alone in the world in exercising jurisdiction over its citizens no matter where they might be. FATCA is intended to detect and deter tax evasion by U.S. citizens through the use of accounts held abroad. But the extraterritorial feature is that FATCA places the reporting burden primarily on financial institutions, wealth managers, and national tax authorities, rather than individuals. These are foreign entities. For example in the UK, information on U.S. citizens' accounts holding more than $50,000 must be reported to HM Revenue & Customs, who will then pass details to the U.S. Internal Revenue Service (this latter step is the subject of a bilateral agreement between the U.S. and the UK).

---

33. *In re* Vitamin C Antitrust Litig., 810 F. Supp. 2d 522, 541 (E.D.N.Y. 2011) (quoting Karaha Bodas Co., L.L.C. v. Perusahaan Pertambangan Minyak Dan Gas Bumi Negara, 313 F.3d 70, 92 (2d Cir. 2002)).

34. Brief for Amicus Curiae Ministry of Commerce of the People's Republic of China in support of Defendants-Appellants at 13, *In re* Vitamin C Antitrust Litig., No. 13-4791 (2d Cir. April 14, 2014), ECF No. 105.

Placing responsibility for compliance with the U.S. statute on foreign banks or other such institutions amounts to extraterritoriality writ large. The U.S. was and is able to engage in this kind of regulatory hegemony because it controls the world's finance system, at least for now. Americans, who are mostly unconnected with the international community, probably neither know nor care much about this. But outside the U.S., and in the business and financial community especially, FATCA (and other American regulatory provisos) are controversial. As Felix Salmon put it in the *Financial Times* last year:

> America is using its banking laws not to make its financial system safer, nor to protect its own citizens from predatory financial behaviour, but rather to advance foreign policy and national security objectives. Only in America, for instance, would citizens have to apply to the finance ministry in order to get a visa to visit Cuba.
>
> Leadership is important, and most countries would be fine with following America's lead for some things—cross-border rules governing stability, liquidity, and leverage, for instance. But even then the US has a tendency to ignore everybody else once the rules have been written, and decide to implement a set of entirely separate rules instead. The hegemon does whatever it wants, for its own, often inscrutable reasons, and it does not enjoy being questioned about its decisions.
>
> No other country can get away with this: what we are seeing is unapologetic American exceptionalism, manifesting as extraterritorial powermongering. Using financial regulation as a vehicle for international power politics is extremely effective. It

> is also very cheap, compared with, say, declaring war.
>
> US officials never apologise for the fact that their own domestic law always trumps everybody else's; rather, they positively revel in it. The consequence is entirely predictable: a very high degree of resentment at the way in which the U.S. throws its weight around.[35]

The U.S. indictments, plea agreements and extradition requests in the Fédération Internationale de Football Association (FIFA) fraud scandal are triggering similar signs of international skepticism. The first criticism actually came from Russia,[36] which does not have much credibility in complaining about extraterritorial assertion of power, much less in complaining about the FIFA investigations (since it allegedly benefitted from the bribes that are being investigated). But that does not necessarily detract from the merits of the Russian criticism. Indeed, *The Economist* noted that Russia was onto something, observing that "American prosecutors . . . do indeed reach much farther than their peers elsewhere—sometimes too far" and that while the crack down on FIFA is welcome "when it comes to bribery, America has sometimes been too audacious."[37] DOJ's reliance

35. Salmon, *supra* note 19.

36. *Russia Accuses US of Illegal Overreach with FIFA corruption Indictments*, THE GUARDIAN (May 27, 2015), http://www.theguardian.com/football/2015/may/27/russia-accuses-us-overreaching-fifa-corruption-indictments.

37. *The World's Lawyer: Why America, and not another country, is going after FIFA*, THE ECONOMIST (June 6, 2015), http://www.economist.com/news/international/21653613-why-america-and-not-another-country-going-after-fifa-worlds-lawyer.

on the RICO Act and Travel Act (rather than anti-bribery statutes) to establish jurisdiction to prosecute what essentially are bribery allegations does not help its cause.[38]

The extraterritorial adventures of U.S. courts in antitrust proceedings have not yet produced quite this much heat, but they are producing in their own way a great deal of heat, and one senses that the temperature is rising.

III. INTERNATIONAL COMITY: WHAT IT MEANS AND HOW IT EVOLVED

The complaints by foreign allies about the extraterritorial assertion of U.S. laws all amount to pleas for greater adherence to international comity. The concept of international comity has existed for hundreds of years, but its meaning and purposes have evolved over time as geopolitical circumstances have changed. Notably, it has been shaped, in part, by wars and slavery, which is a reminder of how important the concept of comity is.

International comity doctrine originated on the European continent, where it still appears to command more adherence than in other parts of the world and especially than in the United States. It was first coined by seventeenth century Dutch legal scholars. They were looking for a conflicts-of-law principle that emphasized sovereign independence after the Dutch provinces had finally gained their independence from the brutal Spanish rule after decades of war. Northern Dutch legal scholar Ulrich Huber used the term "comitas gentium" (civility of nations) to describe the following principle: "Sovereigns will so act by way of comity that rights acquired within the limits of a government

38. *Id.*; *see also* Noah Feldman, *U.S. Treats FIFA like the Mafia*, BLOOMBERGVIEW (May 27, 2015), http://www.bloombergview.com/articles/2015-05-27/u-s-treats-fifa-like-the-mafia.

retain their force everywhere so far as they do not cause prejudice to the powers or rights of such government or of their subjects."[39] The basis for his principle was one of mutual respect among states of each other's sovereignty, which he metaphorically described as the high powers of sovereigns offering each other a helping hand.[40]

Notably, this discretionary concept of comity flowed from the then already well-established starting point that the laws of each state were limited to the territory of that state and had no force outside it.[41]

About a century later, it was slavery that brought comity to the forefront in the Anglo-American world. In *The Case of James Sommersett*, a British judge, following Huber's discretionary concept of comity, refused to apply U.S. slavery laws and freed a slave traveling in the United Kingdom with his U.S. slaveholder because slavery conflicted with British policy.[42] He held that comity did not require recognition of U.S. slavery laws because slavery was "incapable of being introduced on any reasons, moral or political."[43] Unfortunately, comity's objective to encourage reciprocal respect and help diplomatic relations led to the opposite outcome in the United States. In its infamous *Dred Scott* opinion, the Supreme Court stated:

> [n]ations, from convenience and comity, and from mutual interest, and a sort of moral necessity to do justice, recognize and administer the laws of other

---

39. Ernest G. Lorenzen, *Huber's De Conflictu Legum*, 13 ILL. L. REV. 375, 376 (1919), *available at* http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5566&context=fss_papers.

40. ULRICH HUBER, HEEDENSDAEGSE RECHTSGELEERTHEYT 13 (1699).

41. Lorenzen, *supra* note 39, at 376.

42. The Case of James Sommersett, 20 How. St. Tr. 1, 3-4 (K.B. 1772).

43. *Id*.

> countries. But, of the nature, extent, and utility, of them, respecting property, or the state and condition of persons within her territories, each nation judges for itself; and is never bound, even upon the ground of comity, to recognize them, if prejudicial to her own interests. The recognition is purely from comity, and not from any absolute or paramount obligation.[44]

Similar to *Sommersett*, the Court in *Dred Scott* suggested a discretionary comity test balancing foreign against domestic interests, but the laws of the slave states won out. Ultimately, this application of comity did not foster enough respect to avoid the Civil War.

The still-prevailing Supreme Court definition of comity came later, in 1895, in *Hilton v. Guyot*.[45] There, Justice Gray explained and defined comity as follows:

> No law has any effect, of its own force, beyond the limits of the sovereignty from which its authority is derived. The extent to which the law of one nation, as put in force within its territory . . . shall be allowed to operate within the dominion of another nation, depends upon what our greatest jurists have been content to call 'the comity of nations.' . . .
>
> 'Comity,' in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to

44. Dred Scott v. Sandford, 60 U.S. 393, 460 (1856).

45. 159 U.S. 113 (1895).

> international duty and convenience, and to the rights of its own citizens, or of other persons who are under the protection of its laws.[46]

The *Guyot* Court's international comity analysis was thus still very similar to Huber's original articulation. However, the *Guyot* Court appeared to give less discretion to and impose greater duty on the courts to give due regard to foreign sovereigns' laws than Huber had originally envisioned.

That said, the *Guyot* Court ultimately concluded that, in this case, "the comity of our nation" did not require U.S. courts "to give conclusive effect to the judgments of the courts of France" because there was a "want of reciprocity, on the part of France"; the Court determined that French civil procedure did not require French courts to give conclusive effect to an equivalent U.S. (or other foreign) court judgment.[47] This reemphasized that reciprocity is a key characteristic of international comity. That is important to keep in mind as the U.S. asserts its laws and jurisdiction extraterritorially, because foreign nations will view reciprocity as a justification to likewise assert their laws and jurisdiction extraterritorially.

As international trade increased dramatically in the twentieth century, the rule that historically had underpinned the discretionary principle of international comity—that a sovereign nation's law cannot *by its own force* have effect beyond that sovereign's borders—started to loosen in the United States.

For example, in 1909, the Supreme Court still held in *American Banana Co. v. United Fruit Co.* that the U.S. antitrust laws did not apply to conduct outside the U.S. (in Latin America), based on "the general and almost universal rule . . . that the character of an act as lawful or unlawful must be determined

---

46. *Id*. at 163-64.

47. *Id*. at 210.

wholly by the law of the country where the act is done."[48] It explained, "[i]n the case of the present statute, the improbability of the United States attempting to make acts done in Panama or Costa Rica criminal is obvious."[49] But then, in 1945, the Second Circuit (designated by the Supreme Court as the court of last resort) held in *United States v. Aluminum Co. of Am.* (*ALCOA)* that even conduct that occurred abroad was subject to U.S. antitrust laws if it had an intended (anticompetitive) effect in the United States.[50] The extraterritorial nature of the U.S. antitrust laws has since been codified in the Foreign Trade and Antitrust Improvements Act (FTAIA).

As a result, while courts traditionally had applied principles of comity primarily in deciding whether to apply foreign law or recognize foreign judgments in cases involving foreign parties, in the twentieth century courts increasingly started to consider principles of comity in deciding whether to extend domestic law to foreign conduct. The comity principle they applied, however, continued to be essentially the same one as Huber and the *Guyot* Court had originally envisioned.

Over time, U.S. courts collectively have developed the following factors to operationalize international comity in deciding whether to allow extraterritorial application of U.S. law:

> (a) the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory; (b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible

48. 213 U.S. 347, 356 (1909).

49. *Id*. at 357.

50. 148 F.2d 416, 444 (2d Cir. 1945).

> for the activity to be regulated, or between that state and those whom the regulation is designed to protect; (c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted[;] (d) the existence of justified expectations that might be protected or hurt by the regulation; (e) the importance of the regulation to the international political, legal, or economic system; (f) the extent to which the regulation is consistent with the traditions of the international system; (g) the extent to which another state may have an interest in regulating the activity; and (h) the likelihood of conflict with regulation by another state.[51]

As discussed in the next sections, however, courts have applied these factors inconsistently and, thus, have reached widely different conclusions about comity and the extraterritorial reach of U.S. statutes. This has led the U.S. Government and Plaintiffs bar to push the envelope in pursuing extraterritorial cases.

IV. JUDICIAL RESTRAINT AND COMITY: A SOMETIMES THING

U.S. courts have periodically cautioned restraint in extraterritorial application of U.S. laws and sometimes even exercised it. But there do not seem to be many rules that are consistently applied, although this might well be changing.

More than 40 years ago, the Supreme Court stated, "[w]e cannot have trade and commerce in world markets and international waters exclusively on our terms, governed by our laws,

---

51. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403(2) (AM. LAW INST. 1987).

and resolved in our courts."[52] The Court thus bound parties to contracts that conflicted with U.S. laws when a foreign country's interest in the matter outweighed U.S. interests, even if there was some contact in the matter with the United States.[53] Thereafter, the court followed this principle in compelling the parties to arbitrate disputes in antitrust and securities cases that previously were almost certainly have been subjected to private litigation in the courts of the United States.[54] These cases did not explicitly invoke principles of international law or comity, but they reflected a practical and very real view about the limits of the proper reach of American courts.

However, in 1993, the Court went in a somewhat different direction in holding that there must be a true conflict between domestic and foreign law (such that foreign law requires the conduct that is illegal under U.S. law) for a comity issue to exist. In *Hartford Fire Insurance Co. v. California*,[55] the actions by reinsurers in the United Kingdom that led to the antitrust claim under U.S. law were not illegal but also not required under British law; therefore, the Court held, there was no need for a comity analysis because the company could have legally changed its behavior in Britain to avoid breaking U.S. antitrust laws.[56] The decision thus allowed for domestic liability to be imposed under U.S. law even where a defendant was acting quite lawfully in its

52. M/S Bremen v. Zapata Off-Shore Co., 407 U.S. 1, 9 (1972).

53. *Id*. (binding parties to a forum selection clause unless the plaintiff can meet a heavy burden of showing the contract to be unreasonable, unfair, or unjust).

54. *See* Scherk v. Alberto-Culver Co., 417 U.S. 506 (1974) (binding the plaintiff to an arbitration clause in a securities fraud suit when a U.S. purchaser bought securities, but the sale mostly took place overseas); Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc., 473 U.S. 614 (1985) (applying an arbitration clause that conflicted with U.S. law).

55. 509 U.S. 764 (1993).

56. *See id*. at 798.

home country under local law. In his partial dissent, applying the comity factors of the Restatement listed above, Justice Scalia concluded that it was "unimaginable that an assertion of legislative jurisdiction by the United States would be considered reasonable" in this case given that Great Britain "clearly ha[d] a heavy interest in regulating the activity" of the British reinsurer defendants. It was therefore not appropriate, according to Scalia, to assume that Congress had intended such assertion of legislative jurisdiction.[57]

Hartford Fire reiterated what the Second Circuit had held in *ALCOA*: "the Sherman Act applies to foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States."[58] It held that the London reinsurers' express purpose to affect the United States commerce and the substantial nature of that effect outweighed the conflict with British law and required the court's exercise of jurisdiction.[59] This was the result that the British government argued against in an *amicus* filing. Of course, more than a decade prior to the *Hartford Fire* decision, in 1982, Congress had enacted the FTAIA, which provided that the Sherman Act applied to foreign trade or commerce that has a "direct, substantial, and reasonably foreseeable effect" on domestic commerce.[60] There was therefore also a statutory basis for the Court's holding in *Hartford Fire* that permitted it to avoid dealing with comity in any particular depth.

But a decade later, Justice Scalia's reasoning prevailed in *F. Hoffmann-La Roche Ltd. v. Empagran S.A.*[61] Foreign plaintiffs

57. *Id*. at 817-20 (Scalia, J., dissenting).

58. *Id*. at 796.

59. *Id*. at 797.

60. 15 U.S.C. § 6a(1) (2012).

61. 542 U.S. 155 (2004).

had brought a class action suit under the Sherman Act against foreign defendants who had conspired to fix prices in a world-wide market for vitamins. In those circumstances, the comity principles dictated the Court's holding that no domestic claim was cognizable because foreign conduct independently caused foreign harm that alone gave rise to the plaintiff's claim.[62] Insofar as comity principles are concerned, the central notion of the case was that the statute had to be read consistently with the principles of comity to avoid offending foreign sovereigns.[63] The significance of the case is amplified when one appreciates that the foreign conduct did indeed have a significant effect on U.S. commerce, although one that was independent of the effect on foreign commerce. As Justice Kennedy put it, writing for the majority, the rule of statutory construction that had been advanced by Justice Scalia (to the effect that an act of Congress should never be construed as violating international law if any other possible interpretations are available):

> cautions courts to assume that legislators take account of the legitimate sovereign interests of other nations when they write American laws. It thereby helps the potentially conflicting laws of the nation's work together in harmony—a harmony particularly needed in today's highly independent commercial world.[64]

---

62. *Id*. at 159-60. This "gives rise to" language echoes the language of the FTAIA and at the same time has strong parallels with the body of law involving "antitrust injury." In other words, the foreign conduct that violates U.S. law must "give rise to" an unlawful domestic effect in order to be actionable. This principle became much more explicit quite recently in the Seventh Circuit's decision in *Motorola*, discussed *infra.*

63. *Id*. at 164.

64. *Id*. at 164-65.

This brings us to some circuit courts, which have their own history of elasticity and inconsistency when it comes to extraterritoriality. It is useful to begin with the 2012 en banc decision of the Seventh Circuit in *Minn-Chem, Inc. v. Agrium Inc*.[65] The case involved a private treble damage price-fixing class action by purchasers of potash against several Canadian, Russian, or Belarusian potash producers. For present purposes, the pertinent part of the decision involves the meaning of the word "direct," under the FTAIA. In the context of construing the Foreign Sovereign Immunities Act, the Supreme Court had earlier held that an effect is "direct" if it "follows as an immediate consequence of the defendant's . . . activity."[66] A divided panel of the Ninth Circuit embraced this definition as applying to the FTAIA.[67] The Seventh Circuit disagreed and adopted the interpretation urged by the Antitrust Division of the DOJ and the Federal Trade Commission in an amicus brief,[68] holding that the term "direct" in the FTAIA means merely a "reasonably proximate" causal nexus.[69]

---

65. 683 F.3d 845 (7th Cir. 2012).

66. *Id*. at 856 (citations omitted).

67. United States v. LSL Biotechs., 379 F.3d 672 (9th Cir. 2004).

68. Brief for United States and the Fed. Trade Comm'n as Amici Curiae in Support of Neither Party on Rehearing En Banc at 8, Minn-Chem, Inc. v. Agrium Inc., 683 F.3d 845 (7th Cir. 2012) (No. 10-1712), 2012 WL 6641190.

69. *Minn-Chem*, 683 F.3d at 857. Thus construing the words resulted in conduct excluded from the reach of U.S. law being "recaptured" where the U.S. effect could be seen to be "direct [reasonably proximate], substantial, and reasonably foreseeable." This expansion of the exception (coupled with the fact that the statute is no longer seen as limiting the subject matter jurisdiction of the court) has amplified the uncertainty involved and is in part the source of international friction.

But just this year, the Seventh Circuit, in *Motorola Mobility LLC v. AU Optronics Corp.*,[70] took something back from what it appeared to have given in *Minn-Chem*, based in part on considerations of "soft" comity. Once again, the issue of extraterritoriality arose in the context of the FTAIA. The *AU Optronics* panel, in an opinion authored by Judge Posner, limited the reach of the Sherman Act for a variety of reasons, among them because extraterritorial application of American antitrust law in that case would create "friction" with many foreign countries and hence be in conflict with the objectives of the FTAIA.[71] There were, to be sure, other dispositive grounds for the panel's ruling, including that the foreign conduct did not "give rise to" an anticompetitive effect in the United States. Nonetheless, various foreign governments made amicus filings, and the panel was plainly sensitive to the comity issue.

Extraterritoriality and comity have not only featured at the Supreme Court in antitrust cases. The Court has taken up these issues in a number of different contexts, and seems much focused on it as of late. For example, just last year, in *Daimler AG v. Bauman*,[72] the Court relied upon principles of comity in reversing the Ninth Circuit and finding a lack of general jurisdiction over a German corporation. The Court chastised the lower court for insufficiently taking into account considerations of international comity, stating that: a "foreign governments' objections to some domestic courts' expansive views of general jurisdiction have in the past impeded negotiations of international

70. 775 F.3d 816 (7th Cir. 2015), *cert. denied*, No 14-1122, 2015 WL 1206313.

71. *Id*. at 824 (stating "rampant extraterritorial application of US law 'creates a serious risk of interference with a foreign nation's ability independently to regulate its own affairs'" (quoting F. Hoffman-La Roche Ltd. v. Empagran S.A., 542 U.S. 155, 165 (2004))).

72. 134 S. Ct. 746 (2014).

agreements on the reciprocal recognition and enforcement of judgments."[73] Nearly three decades earlier, in *Asahi Metal Indus. Co. v. Superior Court of California, Solano Cnty.*, the Supreme Court had similarly warned state courts in California to consider the policy interests of foreign nations (and the unique burdens on an alien defendant of litigating in a foreign legal system) when exercising personal jurisdiction over foreign defendants.[74]

Five years ago, the Supreme Court decided *Morrison v. National Australia Bank Ltd.*,[75] a case involving foreign private plaintiffs suing foreign and American defendants under the U.S. Securities Exchange Act of 1934 for damages they suffered from alleged misconduct related to securities traded on foreign exchanges. In holding that the plaintiffs failed to state a claim,[76] the Court reiterated the longstanding but arguably moribund principle of statutory interpretation that American law, unless expressly and clearly stated otherwise, is meant only to apply within the territorial jurisdiction of the U.S.

The Court's ruling against the plaintiffs gave no particular weight to the fact that some of the illegal conduct took place in the United States. It concluded that the 1934 Act was clearly confined to securities traded on a U.S. exchange, noting the risk of interference that extraterritorial application of the 1934 Act would entail given that "the [securities] regulation of other countries often differs from ours as to what constitutes fraud, what disclosures must be made, what damages are recoverable, what discovery is available in litigation, what individual actions

---

73. *Id*. at 763.

74. *See* Asahi Metal Indus. Co. v. Superior Court of California, Solano Cnty., 480 U.S. 102, 115-16 (1987) (reversing the Superior Court of California's finding of personal jurisdiction over a Japanese manufacturer).

75. 561 U.S. 247, 255 (2010).

76. *Id*. at 253, 273.

may be joined in a single suit, what attorney's fees are recoverable, and many other matters."[77]

In 2013, in *Kiobel v. Royal Dutch Petroleum Co.*, the Court held that this same "presumption against extraterritoriality" also applies to claims under the Alien Tort Statute (ATS), because nothing in that statute's text "evinces a clear indication of extraterritorial reach," even though the ATS was meant to cover offenses against the law of nations, including piracy (which inherently occurs outside U.S. territory).[78] Defendants' alleged aiding and abetting of a violent suppression of environmental protests in Nigeria, therefore, was not subject to the jurisdiction of a U.S. court under the ATS, according to the Court.[79]

Notably, these signs of increasing exhortations to judicial restraint seem to be most frequent and applicable in cases involving private actions for civil damages. When criminal conduct is involved, and criminal penalties are involved, the federal courts in this country do not seem to have flinched or shrunk from applying U.S. law against foreign companies and foreign individuals, imposing massive criminal fines on the foreign companies, and throwing foreign citizens in jail. Indeed in *Empagran*, the Court recognized and emphasized that there is a difference between a claim by the Government and a private plaintiff because the government seeks relief to protect the public with broad authority.[80] A somewhat similar distinction is evident in the Seventh Circuit's *Motorola* decision, where the court had little difficulty distinguishing between: (i) the failure of foreign conduct by foreign actors to "give rise to" an anticompetitive domestic effect sufficient to support a private claimant; and

77. *Id*. at 269.

78. 133 S. Ct. 1659, 1666-67, 1669 (2013).

79. *Id*. at 1662-63, 1669.

80. F. Hoffmann-La Roche, Ltd. v. Empagran S.A., 542 U.S. 155, 170-71 (2004).

(ii) the ability of the DOJ to prosecute that same conduct in federal courts. [81] The Ninth Circuit held that the same conduct in the same company (AU Optronics) also imported the government's successful criminal prosecution.[82] The Supreme Court denied certiorari in both cases.[83]

The fact that the Court has also addressed comity in the context of discovery is yet another indication that the Court has a noticeable concern about international relations in private damages cases. Nearly twenty years ago, in *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa*, the Court urged respect for international considerations grounded in comity in international discovery, indicating that trial courts should draw a line between reasonable and unreasonable discovery based on the interests of the parties and governments involved. It held that international discovery issues require courts to exercise special vigilance to protect foreign litigants.[84]

V. THE DOJ SEEMS INCLINED TO PUSH THE COURTS TOWARDS AN EXPANSIVE VIEW OF ITS OWN AUTHORITY

Notwithstanding complaints from foreign allies, and notwithstanding the periodic urgings from the Supreme Court and some of the circuits for judicial restraint, the built-in and largely inherent incentives of all of a majority of the parties point in the other direction.

---

81. *See* Motorola Mobility LLC v. AU Optronics Corp., 775 F.3d 816, 825 (7th Cir. 2015).

82. United States v. Hui Hsiung, 778 F.3d 738, 760 (9th Cir. 2015), *cert. denied*, No. 14-1121, 2015 WL 1206283 (U.S. June 15, 2015).

83. *Motorola*, 775 F.3d 816, *cert. denied*, No. 14-1122, 2015 WL 1206313 (U.S. June 15, 2015); Hui Hsiung, 778 F.3d 738, *cert. denied*, No. 14-1121, 2015 WL 1206283 (U.S. June 15, 2015).

84. 482 U.S. 522, 544-46 (1987).

As we have mentioned, private plaintiffs (both foreign and domestic) and their counsel have no interest in complex policy matters such as comity or extraterritoriality. They seek to utilize the vast benefits of the American legal system for the pecuniary gain that the system offers to clients and counsel alike. The calculus for them is quite simple. The greater the extraterritorial reach of U.S. law, the greater: (i) the plaintiffs' class; (ii) the magnitude of their damage claims; (iii) the group of defendants (and thus the plaintiffs' recovery potential); and (iv) the costs and burdens on defendants associated with discovery. Even if the extraterritorial claims are weak, the size of the claim, the uncertainty of jury trials, and the costs associated with discovery help force a greater settlement amount, and thus a greater fee for the lawyers.

As Judge Posner put it in *Motorola II*:

> [t]he position for which Motorola contends would if adopted enormously increase the global reach of the Sherman Act, creating friction with many foreign countries and resentment at the apparent effort of the United States to act as the world's competition police officer, a primary concern motivating the Foreign Trade Antitrust Improvements Act. It is a concern to which Motorola is—albeit for understandable financial reasons—oblivious.[85]

Much the same might be said of the DOJ in this country. The criminal fines and civil penalties collected by the executive branch of our government are enormous in antitrust, False

85. *Motorola*, 775 F.3d at 824 (7th Cir. 2015) (internal citations and quotations omitted).

Claims Act proceedings, RICO actions, London Interbank Offered Rate (LIBOR) and Foreign exchange market (Forex) machinations, and otherwise.

Institutionally, DOJ is much better placed than private plaintiffs and their counsel to consider international comity in deciding what cases and targets to prosecute and what sentences to seek. As part of the Executive Branch, the impact of its enforcement efforts on international relations should matter in its exercise of prosecutorial discretion. Indeed, DOJ has long had in place Antitrust Enforcement Guidelines for International Operations, in which it explains that it considers international comity when enforcing the U.S. antitrust laws extraterritorially, among others, by determining whether enforcement objectives can be achieved by deferring to foreign governments instead.[86] And there is, for example, an agreement between the U.S. and European Communities[87] under which they basically have agreed that the DOJ and European Commission (EC) will normally defer or suspend their own enforcement efforts in favor of the other's where the anticompetitive conduct may have an impact in its own territory but is primarily taking place in and directed at the other's territory.[88]

In actual practice, however, there is little visible evidence that international comity is a significant consideration for DOJ. As the nation's federal prosecutor, the DOJ—and especially its

86. U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST ENFORCEMENT GUIDELINES FOR INT'L OPS. § 3.2 (Apr. 1995).

87. U.S. Dep't of Justice, Agreement Between the Government of the United States of America and the European Communities on the Application of Positive Comity Principles in the Enforcement of Their Competition Law (June 4, 1998), *available at* http://www.justice.gov/atr/agreement-between-united-states-and-european-communities-application-positive-comity-principles.

88. *Id*. Art. IV(2).

prosecuting staff—usually seems singularly focused on securing guilty pleas, convictions, and large fines, including in a great many cases from foreign corporations and citizens. Its aggressive enforcement against overseas conduct and its advocacy efforts before courts in favor of an expansive view of the extraterritorial reach of U.S. laws[89] suggest that considerations of international comity typically take a backseat to enforcement and deterrence, if those considerations get a seat at all.

For example, in *Morrison v. National Australia Bank Ltd.*, the Solicitor General (part of the DOJ) argued for an interpretation that would have had the 1934 Exchange Act extend to fraud related to securities traded on foreign exchanges if the fraud involved conduct in the United States that was material to the fraud's success.[90] The Supreme Court rejected this because there was no express and clear indication by Congress that the 1934 Act applied extraterritorially. Despite *Morrison*, DOJ has continued to prosecute cases extraterritorially where statutes did not provide an express and clear basis for it.

A recent example is *United States v. Sidorenko*.[91] There, the DOJ criminally indicted three foreign nationals for wire fraud and bribery involving a federal program, based on alleged foreign bribery conduct involving a foreign governmental agency (the UN's International Civil Aviation Organization (ICAO) agency). The only link to the U.S. was the fact that the U.S. funds part of ICAO, yet there was no allegation that any of those funds were squandered as a result of the bribes. The Northern District of California dismissed the indictments as an "overreach," explaining that under DOJ's theory:

---

89. *See, e.g.*, Brief for the United States in Opposition, Hsiung v. United States, 778 F.3d 738 (2015) (No. 12-10492), 2015 WL 2353087.

90. 561 U.S. 247, 270 (2010).

91. United States of America v. Sidorenko, No. 3:14-cr-00341, 2015 WL 1814356 (N.D. Ca. Apr. 21, 2015).

> there is no limit to the United States' ability to police foreign individuals, in foreign governments or in foreign organizations, on matters completely unrelated to the United States' investments, so long as the foreign governments or organizations receive at least $10,000 of federal funding. This is not sound foreign policy, is not a wise use of scarce resources, and it is not . . . the law.[92]

The DOJ appealed this decision but then recently decided to drop its appeal.

In *United States v. Chao Fan Xu*, the DOJ secured from a federal court RICO Act convictions, 20-plus year jail sentences, and a $482 million restitution order against four Chinese nationals, based largely on their defrauding of the Bank of China, in China.[93] The link to the U.S. was defendants' use of fraudulently obtained visas and passports to enter the United States and their use of the fraudulently obtained funds to gamble in Las Vegas.[94] The Ninth Circuit held that the RICO Act does not apply extraterritorially given *Morrison*, but nevertheless upheld the convictions because it agreed they were based partly on racketeering activity that occurred in the United States (the immigration fraud).[95] It vacated the district court's sentences (and $482 million restitution order), however, because the court had improperly relied on the defendants' foreign conduct to determine the base offense for the sentences.[96]

In the antitrust context, as discussed above, the DOJ continues to prosecute criminal cases based on cartel conduct and

92. *Id*. at *6.

93. *See* 706 F.3d 965 (9th Cir. 2013).

94. *Id*. at 973.

95. *Id*. at 979.

96. *Id*. at 992-93.

transactions by foreign companies that occur exclusively overseas, on the theory that the cartelized components ultimately find their way into finished products that end up in the United States. The DOJ has been successful in persuading several courts to permit such extraterritorial enforcement of foreign component cartels where it can prove that the U.S. effects of the foreign cartel are sufficiently direct, substantial, and reasonably foreseeable.[97] But in some cases, such as the ongoing auto parts cartel investigations, one may wonder whether such direct, substantial, and reasonably foreseeable effect is present when the price-fixed parts were sold and incorporated in automobiles overseas, and make up but a tiny fraction of the entire value of automobiles that are sold in various countries across the world only one of which is the United States.[98]

In contrast, while the EC recently also reached across borders to penalize overseas cartel sales of components that ended up in finished products sold in the European Economic Area (EEA)—in the same liquid-crystal display (LCD) cartel case as DOJ and Motorola pursued—it did so only to the extent the overseas cartel sales of components were intragroup sales by a company that belonged to the same (vertically-integrated) corporate group that also sold the finished products in the EEA.[99] The European Court of Justice recently blessed that approach.[100]

---

97. *See, e.g.*, United States v. Hui Hsiung, 778 F.3d 738, 758-59 (9th Cir. 2015); Motorola Mobility LLC v. AU Optronics Corp., 775 F.3d 816, 825 (7th Cir. 2015).

98. *Cf*. Hui Hsiung, 778 F.3d at 758 ("the TFT-LCDs are a substantial cost component of the finished products—70-80 percent in the case of monitors and 30-40 percent for notebook computers.").

99. *See* Case C-231/14P, Innolux Corp. v. Commission, ¶¶ 15-16.

100. *Id*. ¶¶ 66-77, 86.

Unlike DOJ, the EC otherwise disregarded purely overseas component cartel sales in calculating its fines.[101]

Perhaps the most notable example of DOJ's expansive position on extraterritoriality can be found in a brief that it filed with the Ninth Circuit in which it took the position that:

> when the Executive Branch, which manages foreign relations, determines that the interests of United States law enforcement outweigh any possible detriment to our foreign relations, and accordingly decides to file a case, separation of powers principles, as well as the Judiciary's own recognition of its limitations in matters of foreign affairs, point to the conclusion that an American court cannot refuse to enforce a law its political branches have already determined is desirable and necessary.[102]

This DOJ position seems extreme. First, it challenges judicial pronouncements from the Supreme Court that we have mentioned above, and second, few litigants, including the DOJ, have any long-term success telling the Judiciary what it cannot do. Specifically, DOJ's position ignores the fact that the legislative branch also ought to have a significant say in international relations, comity, and the extraterritorial reach of U.S. laws—indeed, probably by far the greatest say—and it is the Court's role

---

101. *Id*. ¶¶ 15-16.

102. Reply Brief for Appellant the United States at 23, United States v. LSL Biotechnologies, Inc., 379 F.3d 672 (9th Cir. 2002) (No. 02-16472), 2002 WL 32298182, http://www.justice.gov/file/501546/download (internal citations and quotations omitted); *see also* U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST ENFORCEMENT GUIDELINES FOR INT'L OPS. § 3.2 (Apr. 1995) ("The Department does not believe that it is the role of the courts to 'second-guess the executive branch's judgment as to the proper role of comity concerns under these circumstances.'").

to interpret Congress's legislative intent as to the extent of extraterritoriality when interpreting the statute at hand.[103]

Of course, the DOJ's aggressive extraterritorial assertion of U.S. law in criminal cases inevitably feeds an increase in private suits that reach across borders, since the laws that the DOJ criminally enforces typically also feature a private right of action and since the plaintiffs' bar usually files suit as soon as the DOJ announces an investigation.

As a practical matter, most of the extraterritorial application of U.S. law goes unreviewed. The criminal cases almost never go to trial—virtually all are resolved with plea agreements—and when they do (as in *AU Optronics*) the issues presented are rarely nuanced or focused upon issues that give rise to much of a judicial incentive for restraint. The same is true of most civil cases, apart from the recent Motorola case against AU Optronics in the Seventh Circuit. And in a way, that case was almost a fluke. Motorola won almost every issue in the case throughout the more than five (5) years that it was part of the multidistrict litigation (MDL) proceeding in the Northern District of California. It was only after the case was remanded to the Northern District of Illinois that core issues of the applicability of the FTAIA were revisited.[104]

---

103. Hartford Fire Insurance Co. v. California, 509 U.S. 764, 814-15 (1993) (Scalia, J., dissenting) (quoting Murray v. Schooner Charming Betsy, 2 Cranch 64, 118, 2 L.Ed. 208 (1804) ("An act of congress ought never to be construed to violate the law of nations if any other possible construction remains.")).

104. *See* Briggs, *supra* note 1, at 80-83, for a discussion of the tortured history of that case.

What's more, given the increasingly paramount position of the Judiciary in our system of government,[105] American courts in general also seem to be institutionally disinclined by and large to put limits on the territorial reach of U.S. law, much less their own jurisdiction. Examples of cases showing courts' disinclination to limit their jurisdiction over foreign conduct in foreign lands include the Second Circuit's decisions in recent RICO cases,[106] the D.C. Circuit's first decision in *F. Hoffman-La Roche Ltd. v. Empagran S.A.*,[107] the Ninth Circuit's decision in *Daimler AG v. Bauman*,[108] and the Northern District of California's decision in *In re: TFT-LCD (Flat Panel) Antitrust Litigation (Motorola Inc. v. AU Optronics)*.[109]

In a continuously globalizing economy and a rapidly shrinking commercial world, there is thus a significant and increasing risk that foreign companies and nationals either endure years of costly litigation in the U.S. (with corresponding invasive overseas discovery), or enter costly or painful guilty pleas

---

105. *See* Fukuyama, *supra* note 16, at 11 (discussing the role of U.S. courts transforming from a constraints on government to an instrument for the expansion of government).

106. *See, e.g.*, European Community v. RJR Nabisco, Inc., 764 F.3d 129, 139-43 (2d Cir. 2014) (holding that, despite the presumption against extraterritoriality outlined in *Morrison v. National Australia Bank Ltd.*, the RICO Act reaches extraterritorial conduct to the extent the alleged predicate acts are violations of statutes that expressly have extraterritorial reach).

107. Empagran S.A. v. F. Hoffman-LaRoche, Ltd., 315 F.3d 338 (D.C. Cir. 2003) (holding that purchasers stated a price-fixing claim despite their injuries not arising from U.S. effects of defendants' conduct), *vacated sub nom.* F. Hoffmann-La Roche Ltd. v. Empagran S.A., 542 U.S. 155 (2004).

108. Bauman v. DaimlerChrysler Corp., 644 F.3d 909 (9th Cir. 2011) (finding wholly owned U.S. subsidiary was manufacturer's agent for general jurisdictional purposes), *rev'd sub nom*. Daimler AG v. Bauman, 134 S. Ct. 746 (2014).

109. *In re* TFT-LCD (Flat Panel) Antitrust Litig., 586 F. Supp. 2d 1109 (N.D. Cal. 2008) (finding standing for both direct and indirect purchasers).

or settlements—all in cases that perhaps ought not be governed by U.S. laws or courts but rather by foreign laws, governments, and courts. As and when the world turns, and foreign legal systems begin increasingly to mimic the territorial reach of the American system, the day will come when the executive branch and the legislature might regret what has been allowed to develop.

VI. SCREENS THAT MIGHT RESTRAIN LEGAL IMPERIALISM

The aggressive extraterritorial application of American law has consequences and will have more consequences as time goes on. Some four decades ago we saw the adoption by some of our closest allies of "claw back" and "blocking" statutes, designed to avoid U.S. discovery, block enforcement of U.S. punitive damages awards, and allow claims in their home countries to claw back U.S. punitive damages awards. Now, as detailed above, we are seeing a substantial number of amicus filings by foreign governments in U.S. courts complaining about extraterritorial assertion of U.S. law and jurisdiction.

But more worryingly, we are also seeing other countries follow U.S. practice and increasingly assert their own law extraterritorially, regularly against American and European multinational concerns. Most notably, the PRC has been flexing its muscle overseas, especially in the antitrust arena, when it deems that foreign conduct or transactions by foreign companies threaten its domestic, often state-owned industries. For example, in 2014, MOFCOM, responsible for antitrust reviews of mergers, blocked an international joint venture by three foreign shipping companies (Danish, Swiss, and French shipping companies) based on what many have perceived to be protectionism rather

than antitrust merits;[110] both the U.S. and European antitrust authorities had cleared the joint venture reportedly due to significant associated procompetitive efficiencies.[111] Earlier this year, despite pleas from President Obama not to devalue intellectual property of American companies to the benefit of Chinese firms using U.S. technology,[112] China's National Development and Reform Commission imposed a fine of nearly $1 billion and several licensing restrictions, including a royalty base cap, on Qualcomm for alleged abuse of dominance with respect to standard essential patents and baseband chips.[113]

---

110. *See, e.g.*, *China's shipping alliance rejection underscores protectionist worries*, REUTERS (June 18, 2014), http://uk.reuters.com/article/2014/06/18/china-shipping-competition-idUKL4N0OZ1LK20140618; Melissa Lipman, *China P3 Ban Short On Details But Shows Protectionist Bent*, LAW360 (June 28, 2014), http://www.law360.com/articles/552786/china-p3-ban-short-on-details-but-shows-protectionist-bent; Richard Milne, *China Blocks Proposed Three-way Shipping Alliance*, FIN. TIMES (June 17, 2014), http://www.ft.com/cms/s/0/a9a188be-f60f-11e3-83d3-00144feabdc0.html#axzz3hZwVkPQq.

111. Costas Paris, *Shipping Alliance Set to Make Waves*, WALL ST. J. (Mar. 26, 2014), http://www.wsj.com/articles/SB10001424052702303802104579453252355203622; Foo Yun Chee, *EU regulators clear Maersk, Nippon Yusen shipping alliances*, REUTERS (June 3, 2014), http://uk.reuters.com/article/2014/06/03/uk-eu-containershipping-antitrust-idUKKBN0EE19V20140603; Costas Paris and Clemens Bomsdorf, *Maersk, Partners Surprised by Chinese Regulator*, WALL ST. J. (June 17, 2014), http://www.wsj.com/articles/shipping-alliance-blocked-by-china-1403001240; Clement Tan & Christopher Jasper, *China Blocks European Shipping Pact, Sending Maersk Down*, BLOOMBERG (June 17, 2014), http://www.bloomberg.com/news/articles/2014-06-17/china-rejects-shipping-alliance-application-by-maersk-msc-cma.

112. *See* Michael Martina & Matthew Miller, *As Qualcomm decision looms, U.S. presses China on antitrust policy*, REUTERS (Dec. 16, 2014), http://www.reuters.com/article/2014/12/16/qualcomm-china-antitrust-idUSL3N0TW2SF20141216.

113. Notably, the U.S. Federal Trade Commission and European Commission are also investigating Qualcomm's licensing and business practices, which suggests there could be more international consensus in this case.

But it is not just the PRC. Other countries are also increasingly bold about asserting their laws extraterritorially, sometimes in questionable ways. France, for example, has pushed for European Union privacy laws to create global obligations for U.S. tech companies to remove information from websites, rather than obligations confined to the relevant EU member state territories.[114] A Canadian court recently made a similar, dubious reach across the globe with little consideration for comity, but in a trade secrets case rather than privacy case.[115] These cases touch upon a fundamental constitutional right—freedom of speech—which is treated very differently in different countries. One can and probably should seriously question whether one country should be able censor what information is available to the citizens of another country.

There is no reason to believe that other countries will not follow suit, and this could devolve into a sort of "race to the bottom," especially between the new and old economic superpowers.

Right now, the major difference between the U.S. and other countries asserting their laws extraterritorially is still that

---

114. Mark Scott, *France Wants Google to Apply 'Right to be Forgotten' Ruling Worldwide or Face Penalties*, N.Y. TIMES (June 12, 2015), http://bits.blogs.nytimes.com/2015/06/12/french-regulator-wants-google-to-apply-right-to-be-forgotten-ruling-worldwide/.

115. *See* Equustek Solutions Inc. v. Google, Inc., 2015 BCCA 265 (June 11, 2015) (upholding an order requiring Google, a non-party to the underlying trade secrets dispute, to remove from globally used web properties any search results showing the allegedly infringing products); *see also* Mike Masnick, *Canadian Court: Yes, We Can Order Google To Block Websites Globally*, TECHDIRT (June 12, 2015), https://www.techdirt.com/articles/20150611/13104231311/canadian-court-yes-we-can-order-google-to-block-websites-globally.shtml; Vera Ranieri, *Canadian Court Affirms Global Takedown Order to Google*, ELEC. FRONTIER FOUND. (June 12, 2015), https://www.eff.org/deeplinks/2015/06/canadian-court-affirms-global-takedown-order-google.

most other countries do so primarily through civil or administrative government actions, while the U.S. also does so in criminal actions as well as at the behest of private parties in civil punitive damages suits. But that, too, could change. For example, certain countries are adopting criminal antitrust enforcement regimes as well as systems facilitating civil antitrust damages claims, similar to the U.S. system. Perhaps, therefore, it is not too farfetched to believe that the extraditions, jail sentences, and punitive damages awards at some point will start running the other way, and the U.S. might not like it. This may become particularly worrisome when U.S. companies and their executives engage in global conduct that is considered lawful (and perhaps even beneficial) in the U.S., yet unlawful and perhaps criminal in other countries.

To be sure, not all extraterritorial application of U.S. law and jurisdiction is inconsistent with international comity. In many cases, it may not be.[116] The "effects test" of *ALCOA* and

116. Some argue, for example, that giving too much weight to comity considerations could undermine deterrence and harm U.S. consumers. *See, e.g.*, Joseph E. Harrington, Jr., *The Comity-Deterrence Trade-off and the FTAIA: Motorola Mobility Revisited*, COMPETITION POLICY INT'L (Jan. 2015); Eleanor M. Fox, *Extraterritoriality and Input Cartels: Life in the Global Value Lane—The Collision Course with Empagran and How to Avert It*, COMPETITION POLICY INT'L (Jan. 2015). We agree that deterrence and protection of U.S. consumers is certainly one consideration in the international comity balancing test between domestic interests and foreign interests. But we disagree with the proposition that comity no longer is or should not be a consideration in extraterritorial antitrust cases once a "direct, substantial and reasonably foreseeable effect" on U.S. commerce has been established. In our view, this conclusion misses the point that the DOJ and many U.S. courts find such an effect too easily, without sufficiently considering comity considerations in the first place. What's more, in thinking about deterrence, one should also consider that less extraterritorial overreaching might give foreign nations greater incentives and ability to put in place and enforce their own laws to deter harmful conduct. Finally, the authors' observations (understandably) focus solely

Hartford Fire makes much more sense, and probably gives less offense to comity, where the conduct at issue is similarly unlawful under the law of the foreign jurisdiction in ways that are broadly comparable. But even so, in most cases the remedies are still often different. For example, most foreign governments still do not jail their citizens for price fixing in many of the circumstances that give rise to jail time in United States. Similarly, there is no country in the world with: comparable class-action machinery; treble damages; one way attorney's fees awards; the absence of contribution coupled with joint and several liability; or the vast discovery machinery authorized by Rule 26 of the Federal Rules of Civil Procedure. One might suppose that the incompatibility of these American civil and criminal enforcement regimes would give rise to a more thoughtful restraint being placed upon the American judiciary, but that has not happened.

Our purpose here, and it is but a modest beginning, is to mention a few approaches that might, in the fullness of time and the absence of domestic political dysfunction, become viable. Such screens (which could be managed by the executive, legislative, and judicial branches separately or with the branches of government acting in concert) might include institutionalization of the following types of measures:

---

on antitrust harm and deterrence, while comity is in part about a much bigger picture. In the U.S., we have long considered cartel violations a supreme evil meriting significant jail sentences, fines, and treble damages to root it out as much as possible. Other nations have come somewhat to agree, but have not gone so far as to criminalize cartels, put individuals in jail, award exemplary damages, provide for one way attorney's fees, apply joint and several liability without any right of contribution, or embrace various other features of American antitrust law that make it so controversial outside the borders of the United States. In some ways, comity is about all nations "giving a little" so as to not over-impose their values on one another.

1) The adoption of a rule of prescriptive comity, "the respect sovereign nations afford each other by limiting the reach of their law," along the lines suggested by Justice Scalia in his *Hartford Fire* dissent.[117] In the case of *Hartford Fire*, a prescriptive comity approach would have resulted in the court declining to exercise the Sherman Act extraterritorially because the conduct at issue was regulated under a comprehensive foreign regulatory scheme.[118] This approach would be different from, but quite analogous to, the more familiar State Action doctrine of long-standing vintage in this country.
2) The implementation of rules that guarantee foreign defendants a practicable and meaningful opportunity to raise extraterritoriality and international comity defenses or concerns at the front end of a case, and based on strictly limited discovery. Such an approach might put extraterritoriality concerns much closer to the level of subject matter jurisdiction.
3) A change to the rules of civil procedure so as to avoid remitting these issues, as they are now often remitted, to the vagaries of Rule 26. In FTAIA cases, this was the norm since, until recently, the FTAIA was treated as a limitation on the subject matter jurisdiction of the federal courts. Indeed, that might still be the case in various circuits

117. 509 U.S. 764, 817 (1993) (Scalia, J., dissenting).

118. This approach is the subject of a thoughtful law review note, Stephen D. Piraino, *A Prescription for Excess: Using Prescriptive Comity to Limit the Extraterritorial Reach of the Sherman Act*, 40 HOFSTRA L. REV. 1099, 1128-34 (2012).

where the issue has not been decided.[119] But now that many appeals courts no longer treat the FTAIA as limiting the subject matter jurisdiction of the trial courts, extraterritoriality and international comity defenses do not necessarily get resolved at the front end of a case before discovery commences. Instead, they can be at the back end of the queue. Indeed, in *Motorola*, the defendant was subjected to many years of full discovery before the issue finally was determined.

4) Implement a formal process whereby foreign targets of DOJ investigations are assured of the opportunity to raise extraterritoriality and international comity defenses with an independent, high-ranking DOJ official during the early stages of the investigation, before the pressure to enter a guilty plea becomes unsustainable. That same DOJ official should be obliged to confer also with the appropriate officials of the Department of State.
5) Implement a formal, mandatory, and early-stage process whereby the prosecuting staff of the DOJ must clear extraterritorial enforcement efforts with an independent, high-ranking DOJ official, also obliged to confer with the Department of State, so as to ensure that international comity is given appropriate weight in each exercise of prosecutorial discretion.
6) Where foreign nationals plead guilty to criminal offenses based on non-U.S. conduct the effects of

119. *See, e.g.*, Minn-Chem, Inc. v. Agrium Inc., 683 F.3d 845 (7th Cir. 2012) (en banc) (overturning United Phosphorus Ltd. v. Angus Chemical Co., 322 F.3d 942 (7th Cir. 2003) (en banc), which previously held that the FTAIA proscribes subject-matter jurisdiction).

which are primarily felt outside the United States, there should be a procedure whereby after sentencing these citizens are returned to their home country, which can choose to implement the sentence, or not.

7) Implement a procedural rule whereby the DOJ and courts overseeing private civil punitive or treble damages actions are required to solicit the views of the U.S. government when foreign defendants raise extraterritoriality or international comity defenses or objections.

We are under no illusion that any one of these "screens," or any combination of them, would "solve" a "problem" that many do not recognize as either existing, or being particularly serious if it does exist. But we do think there is a problem inherent in the American legal system that will lead nearly always and ineluctably to the expansion of judicial extraterritorial jurisdiction. The idea of judicial restraint in this area is as admirable as it is chimerical. Many of our judges, state and federal, are not inclined to put limits on their own powers and have relatively little appreciation for international relations. In the absence of some machinery that can supply restraint, and in the absence of enforcement standards with some objective features, the problem will get bigger before it gets smaller. In practical economic terms, the stakes are potentially very high in an increasingly global economy where the United States is neither the only dominant economic power nor the only country with the will to apply its own law in various places around the world.

January 6, 2016

Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks

Recently reported network intrusions and disruptions, thefts of electronic data, and other significant cyber incidents have impacted millions of people and exposed the increased and continuing risks for businesses and government agencies. These incidents have transformed the cyber threat from a theoretical problem into a clear and present danger. In a recent survey of U.S. executives, security experts, and others from the public and private sectors, "76% of respondents said they are more concerned about cybersecurity threats this year than in the previous 12 months."[1]

Cybersecurity has become a priority for lawmakers and law enforcement agencies, regulators and the White House. It has become part of the public consciousness, and across corporate America, the cyber threat has evolved from an information-technology problem that could be delegated to information-technology personnel to a key business and governance risk requiring the careful attention of boards and senior leadership.

In this memo, we: (1) provide an overview of this new reality; (2) address the nature and sources of the cyber threat; (3) discuss the potential financial, legal, and other consequences of cyber incidents; (4) present the legal and regulatory framework applicable to cybersecurity issues; (5) offer best practices and recommendations for boards and senior management; and (6) examine recent resources tailored to the particular cybersecurity risks facing financial institutions.

TABLE OF CONTENTS

Introduction

Cyber-related events during the last several months illustrate the current reality—cybersecurity is a growing business and governance risk that requires immediate and regular attention by business leadership:

- When the operations of the New York Stock Exchange and United Airlines were suddenly halted due to technological glitches, fears of a cyberattack quickly spread. In response, the NYSE issued a statement (on Twitter, no less) assuring the public that the outage resulted from "an internal technical issue and is not the result of a cyber breach."[2] Similar messages were delivered the same day by the White House ("[T]here is no indication that malicious actors are involved in these technology issues."),[3] the Director of the Federal Bureau of Investigation ("FBI") ("We do not see any indication of a cyber breach or a cyber attack."),[4] and the Secretary of Homeland Security ("[T]he malfunctions at United and the stock exchange were not the result of any nefarious actor."), who also reiterated that "cybersecurity is a top priority for me, for the President, and for this Administration."[5]

- The Department of Justice (the "DOJ") announced charges against nine people in connection with an international ring of organized cybercriminals who hacked into the networks of business newswires to steal press releases prior to their public release in order to trade on the stolen inside information.[6]

- Citing the "increasing barrage of cyber attacks on financial firms," the U.S. Securities and Exchange Commission (the "SEC") announced charges last week against a St. Louis-based investment adviser that the SEC alleged had "failed to establish the required cybersecurity policies and procedures in advance of a breach."[7]

- The Director of the U.S. Office of Personnel Management ("OPM") was forced to resign in the wake of a massive data breach that compromised sensitive personal information of millions of federal employees with security clearances.[8]

- *Wired* magazine documented a group of hackers remotely manipulating a vehicle's air conditioning, stereo controls, brakes, and transmission using a laptop miles away, and as *The New York Times* has reported, "[t]hough automakers say they know of no malicious hacking incidents so far, the risks are real."[9] Just days later, Fiat Chrysler announced a recall of 1.4 million vehicles due to "a potential cybersecurity flaw," reportedly prompting an investigation by the National Highway Traffic Safety Administration.[10]

- FBI Director James Comey warned that that the FBI is "picking up signs of increasing interest" among terrorist groups in a cyberattack against the United States.[11]

- The former Superintendent of the New York Department of Financial Services called cybercrime "a huge threat to our financial system" and predicted that there would be "a lot of action around cybersecurity and the regulation in that area."[12]

- The FBI arrested several people in the United States and Israel this summer who, according to several news reports, are linked to a data breach at one of the country's largest banks.[13]

More thought, attention, and resources are being devoted to cybersecurity than ever before. The government has issued extensive guidance addressing cybersecurity, and lawmakers are working to enhance the ability of the public and private sectors to defend against and respond to the cyber threat. The purpose of this memo is to outline the threat, the applicable legal and regulatory framework, and key steps to mitigate the legal and business risks posed by the brave new cyber world. This memo also examines two recent developments of particular relevance to the financial industry: a July 2015 Government Accountability Office ("GAO") Report on cybersecurity at banks and other depository institutions, and the Cybersecurity Assessment Tool recently developed by the Federal Financial Institutions Examination Council ("FFIEC").

As described below, it is essential that businesses—particularly those that collect and transmit business and customer data online—conduct periodic risk assessments; undertake comprehensive preventative measures to fortify defenses; develop effective employee training and education, policies, and controls; and design robust incident response plans to ensure maximum preparedness in the event of a breach. Although the risk of a cyber incident cannot be eliminated, companies can meaningfully mitigate the risk and resulting harm by preparing for an incident before it occurs.

The Nature and Sources of the Threat

According to a February 2015 worldwide threat assessment by the United States intelligence community, "[c]yber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact."[14] The Director of National Intelligence has predicted that "[r]ather than a 'Cyber Armageddon' scenario that debilitates the entire US infrastructure," it is more likely that there will be "an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time."[15] Corporations across a broad spectrum of industries often find themselves the targets of these low-to-moderate level cyberattacks, which can manifest in many different forms.

Likely Business Targets

The financial industry consistently has been one of the sectors most likely to be the target of a cyberattack. According to the 2015 IBM Cyber Security Intelligence Index, the finance industry had the highest incident rate across surveyed industries in 2013 and 2014, accounting for approximately one-quarter of the private-sector incidents observed by IBM during each of those years.[16] That finding is consistent with

those of other cybersecurity providers and researchers. Verizon, for example, reported that among private industries, the financial services industry was second only to the information industry in the number of cyberattacks,[17] and Mandiant identified financial services as one of the top three most targeted industries, together with retail and business and professional services.[18]

The Sources of External Threats

The primary sources of external threats to companies and organizations are: "(1) nation states with highly sophisticated cyber programs (like Russia or China), (2) nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea)," (3) individual or organized cybercriminals who typically act for financial gain, and (4) so-called "hacktivists" who are motivated by ideological objectives.[19]

There is evidence that large banks are "more likely to be targeted by nation-states and hacktivists," while smaller depository institutions, which typically have less sophisticated defense mechanisms, are more commonly targeted by financially-motivated cybercriminals.[20] Financially-motivated cybercriminals traditionally have sought banking credentials, credit card or other personal information from a variety of businesses, but the type of information being targeted—as well as the means of monetizing that information—is expanding. Recently, the DOJ announced the indictment of nine people in a large-scale, international scheme to hack into business newswires, steal yet-to-be published press releases containing confidential financial information, and then illegally trade on the basis of that stolen information.[21] Along similar lines, Mandiant recently profiled the activities of a sophisticated group of cybercriminals who have been targeting confidential M&A information from public companies, presumably to engage in insider trading.[22] In addition, the Director of the FBI expressed growing concern about terrorist groups looking to carry out a cyberattack.[23]

The Blurring of State and Non-State Actors

The lines between state-sponsored and other cyber actors have blurred, as the techniques and motives of cybercriminals and state actors have increasingly overlapped.[24] State actors have expanded beyond traditional espionage and have also "undertaken offensive cyber operations against private sector targets" to advance political, foreign policy or economic objectives, or to seek "retribution for perceived wrongs."[25] North Korea, for example, launched a highly destructive attack against Sony Pictures Entertainment in apparent retaliation for its planned release of a satirical film depicting the assassination of Kim Jong-un.[26] It is widely suspected—although the U.S. has officially declined to confirm—that China was behind the recent OPM hack, which resulted in the theft of sensitive information for millions of federal employees and potentially compromised the identities of intelligence officers secretly stationed abroad.[27] China has also been linked to both a prolonged intrusion at *The New York Times*[28] and the seizing of millions of electronic records held by U.S. health insurer Anthem.[29] Five Chinese military hackers were charged with economic espionage last year for allegedly hacking into the networks of private entities in America to steal

information "that would be useful to their competitors in China, including state-owned enterprises."[30] Then-Attorney General Eric Holder described it as "the first ever charges against a state actor for this type of hacking."[31] It can sometimes be difficult to distinguish between state and non-state actors within the same country when those "varied actors actively collaborate, tacitly cooperate, condone criminal activity that only harms foreign victims, or utilize similar cyber tools."[32]

The Range of External Attacks

The range of objectives motivating cyberattackers has resulted in a range of different types of attacks against businesses. In 2012 and 2013, for example, dozens of financial institutions were subjected to coordinated and sustained distributed denial-of-service, or DDoS, attacks.[33] Those attacks caused disruptions to online banking functions, but resulted in no reported losses of personal information, suggesting a lack of any pecuniary motive.[34] Some government officials and security researchers attributed the attacks to the government of Iran, suggesting the attacks may have been "in retaliation for economic sanctions and online attacks by the United States,"[35] while others have attributed the DDoS attacks to a group of hacktivists in Iran.[36]

In the summer of 2014, one of the largest U.S. banks suffered a data breach that compromised account information belonging to over 80 million households and small businesses.[37] It was reported that customer email addresses, home addresses, and telephone numbers were compromised, but that no customer funds were taken.[38] The DOJ announced arrests this summer of several individuals in the U.S. and abroad who reportedly were linked to this breach.[39]

In two of the largest financially-motivated cyberattacks, in 2013 and 2014, Target and Home Depot were victims of data breaches that involved the theft of credit card data of more than 40 million customers and 56 million customers, respectively.[40] And aside from these large-scale attacks, banks routinely experience so-called "account takeovers" in which cybercriminals surreptitiously obtain victims' banking credentials and then direct wire transfers or other withdrawals from the victims' accounts.[41] The methods used to obtain the victims' banking credentials vary, but often include phishing emails or luring victims into unwittingly installing malware on their computers that enables the perpetrator to steal their banking information.[42]

More recently, healthcare companies—which maintain extensive records of personal information—have become victims of the so-called mega-breaches that had been affecting the retail sector. In February 2015, for example, Anthem, "the second-largest health insurer in the United States," announced that hackers stole information regarding tens of millions of its customers from a database containing up to 80 million customer records.[43]

The Tools of External Attacks

The methods of carrying out these attacks vary in their degree of sophistication. Although certain actors, particularly state-sponsored actors, have become increasingly more sophisticated, phishing and other relatively unsophisticated methods remain common, and employee errors and supply-chain vulnerabilities continue to be responsible for many cyber incidents. The recently-indicted hackers who allegedly stole press releases in order to trade on inside information used phishing emails, among other methods, to infiltrate the networks of the business wires.[44]

Another factor contributing to and compounding the cyber threat is the proliferation of widely-available hacking tools, which increasingly enable virtually anyone, anywhere in the world, to carry out cyberattacks. The DOJ announced criminal charges last year in a case involving the sale of malware to thousands of people around the world who, for only $40, could surreptitiously take over a victim's computer and then spy on their victims through their web cameras, steal files and account information, log victims' key strokes, and utilize the infected computers to carry out DDoS attacks.[45]

Threats From Within

Aside from these sources of external threats, insiders present another source of risk, accounting for more than 50% of cyber incidents by some estimates.[46] Data breaches caused by insiders often can be more inadvertent than malicious.[47]

Further highlighting the vulnerabilities created by employees, data collected from sanctioned tests involving the distribution of over 150,000 phishing emails "showed that nearly 50% of users open e-mails and click on phishing links within the first hour" of receiving them.[48] This has important implications for the design of cybersecurity programs, reinforcing the need to incorporate effective employee training and education into any cybersecurity program. This is addressed in more detail below.

Financial, Legal and Other Implications of Cyber Incidents

The direct financial costs resulting from a significant cyber incident can be substantial. Target, for example, reported that as of May 2, 2015, it had incurred $256 million in data-breach expenses since its 2013 data breach in which hackers stole the credit card information of millions of customers.[49] Sony estimated that the breach of its PlayStation Network, which compromised the information of millions of users, would cost the company more than $170 million,[50] and the Sony Pictures Entertainment hack in connection with the film "The Interview" was projected to cost the company hundreds of millions of dollars, including lost revenue from the decision to pull the film's release from theaters.[51]

Victim companies also face litigation risks and intangible and less-quantifiable harms, including reputational damage, loss of consumer confidence, disruption of business operations, destruction of files, drops in stock price, and even the potential for embarrassment—such as when personal emails are released to the public by hackers.[52]

Private Litigation Risks

In the wake of a significant cyber incident, companies—and their directors and officers—can face a flurry of private lawsuits from a range of different constituencies: individual consumers whose personal information has been compromised, shareholders alleging failures by the board and senior leadership in preparing for and/or responding to cyberattacks, and other third-parties potentially affected by a breach, such as banks and credit card companies.

Target, for example, faced dozens of lawsuits after the data breach that compromised the credit/debit card and other personal information belonging to as many as 100 million consumers. As in other breach cases, the consumer-plaintiffs asserted violations of state consumer protection and state data-breach statutes, as well as common law claims of negligence, breach of implied contract, bailment, and unjust enrichment.[53] The plaintiffs' factual allegations related to the company's conduct pre- and post-breach, including, for example, that Target allegedly failed to (1) "take adequate and reasonable measures to ensure its data systems were protected," (2) "take available steps to prevent and stop the breach from ever happening," (3) "disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' financial account and personal data," and (4) "provide timely and adequate notice of the Target data breach."[54]

The multi-district consumer litigation was consolidated in the District of Minnesota, and in March 2015, following the denial of the defendant's motion to dismiss, the District Court preliminarily approved a settlement of the consumer litigation.[55] The proposed settlement requires Target to pay $10 million to consumers who used credit or debit cards at Target during the relevant time period and to implement various security measures to protect customer data, including: appointing a chief information security officer, creating metrics to track and maintain information security, and offering security training to its employees.[56]

According to published reports, Target subsequently reached a proposed $19 million settlement to reimburse financial institutions for the costs they incurred from the breach, such as reimbursing fraudulent charges and reissuing credit and debit cards.[57] The financial institutions had alleged violations of a Minnesota credit-card statute, negligence, and negligent representation by omission for failing to disclose information-security weaknesses. The settlement was derailed in May of this year, however, after failing to receive the required 90% participation rate from issuers.[58] In August, Target reached a settlement with Visa Inc. and the banks that issue Visa cards for up to $67 million.[59] Another group of

financial institutions was recently certified as a class in federal court in the District of Minnesota, allowing other financial institutions the opportunity to join the suit against Target.[60]

Derivative shareholder litigation against Target's directors remains pending.[61] The shareholder plaintiffs have asserted claims for, among other things, breach of fiduciary duty, waste of corporate assets, and gross mismanagement, and like the consumer plaintiffs, they rely on allegations concerning the defendants' supposed pre-breach failure to insure adequate safeguards and their post-breach response.[62]

Risks of Enforcement Proceedings or Public Inquiries

In addition to private lawsuits from these various constituencies, companies that are victims of a cyber incident can also face investigations and enforcement actions from a wide array of federal and state regulators and law enforcement agencies, as discussed in greater detail below. Cybercrime creates a somewhat unique situation in which a company that is a victim of an attack may at the same time be viewed by regulators as a subject of a government investigation. In the case of a significant breach, the possibility also exists that a company may be the subject of a Congressional inquiry and its executives could be called to testify.[63]

Risks to Senior Leadership

The recent wave of cyberattacks also has placed great pressure on organizations to hold management accountable for perceived lapses. Last year, Target's board of directors ousted the company's CEO following its data breach, marking the first time a CEO has been removed due to a cyber incident.[64] In addition, Institutional Shareholder Services ("ISS") took the unusual step of recommending that Target shareholders vote against seven of the ten directors (focusing on those who served on the audit and corporate-responsibility committees) for taking insufficient steps to ensure that Target's systems were fortified against security threats.[65] And the director of the OPM was forced to resign this summer in the wake of a massive data breach that compromised the personal information of more than 20 million federal employees.[66]

These consequences have served to reinforce the warning from one SEC Commissioner that "boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."[67]

Regulatory Requirements and Enforcement Priorities

A wide variety of federal and state regulators and law enforcement agencies are increasingly directing their attention toward cybersecurity. The DOJ, SEC, Financial Industry Regulatory Authority ("FINRA"), Federal Communications Commission ("FCC"), U.S. Department of Health & Human Services ("HHS"), Federal Trade Commission ("FTC"), a number of state attorneys general, and federal bank regulators have enhanced

their emphasis on cybersecurity and, in many cases, specifically identified cybersecurity as a priority. Organizations across sectors should therefore expect both increased rulemaking and enforcement activity.

The U.S. Department of Justice and Federal Law Enforcement Agencies

A number of federal agencies charged with law enforcement and prosecution have increasingly focused on cybersecurity and have dedicated significant resources to pursuing and prosecuting cybercrime. The Criminal Division of the DOJ created the Cybersecurity Unit within the Computer Crime and Intellectual Property Section in December 2014 "to serve as a central hub for expert advice and legal guidance regarding how the criminal electronic surveillance and computer fraud and abuse statutes impact cybersecurity."[68] In April 2015, the Cybersecurity Unit released its recommended Best Practices for Victim Response and Reporting of Cyber Incidents "to assist organizations in preparing a cyber incident response plan and, more generally, in preparing to respond to a cyber incident."[69] The Cybersecurity Unit also is "helping to shape cyber security legislation" and "engag[ing] in extensive outreach to the private sector to promote lawful cybersecurity practices."[70] In addition to the Cybersecurity Unit, many U.S. Attorney's Offices across the country have allocated resources to investigating and prosecuting cybercrime.

The FBI has identified cybersecurity as one of the agency's top three priorities, and has instituted a "set of technological and investigative capabilities and partnerships" to assist in its efforts to combat cybercrime, including: a Cyber Division, "[s]pecially trained cyber squads at FBI headquarters and in each of [the] 56 field offices," cyber action teams, 93 Computer Crimes Task Forces, and partnership with other federal agencies such as the Department of Defense and Department of Homeland Security.[71] The U.S. Secret Service, within the Department of Homeland Security ("DHS"), maintains a national network of more than 35 Electronic Crimes Task Forces with a "focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes."[72]

Federal prosecutors have recently brought a number of significant criminal cases targeting cybercrimes. Federal prosecutors announced charges last month against nine stock traders and computer hackers who allegedly reaped as much as $100 million in illegal insider-trading profits "by conspiring to use information stolen from thousands of corporate press statements before their public release."[73] A month earlier, the DOJ announced that it had dismantled a major computer hacking forum called Darkode and charged 12 people associated with the forum.[74] Domestic law enforcement efforts to combat cybercrime have benefitted from an extraordinary degree of international cooperation rarely seen in other contexts. The Darkrode case, for example, was part of a coordinated effort by law enforcement authorities from 20 different countries, representing "the largest coordinated international law enforcement effort ever directed at an online cyber-criminal forum."[75] Similarly, the U.S. Attorney's Office in Manhattan brought charges last year in connection with the sale and use of "Blackshades" malware as part of a global law enforcement operation involving more than 90 arrests and other law enforcement actions in 19 countries.[76]

U.S. Securities & Exchange Commission

While SEC officials have at various times hinted at the prospect of additional cyber-related enforcement actions, the director of the SEC's Chicago Regional Office recently emphasized that "[c]ybersecurity . . . is an area where we have not brought a significant number of cases yet, but is high on our radar screen."[77] He pointed to two areas in particular on which the SEC is focused: cybersecurity controls and cyber-related disclosures.[78]

SEC Guidance for Public Companies

On the disclosure side, the SEC's Division of Corporation Finance (the "Corp Fin Division") has issued "disclosure guidance" to aid public companies in their cyber-related disclosures.[79] The guidance first addresses the potential disclosure of cybersecurity as a significant risk factor. In determining whether the risk rises to that level, companies should consider "prior cyber incidents and the severity and frequency of those incidents," as well as "the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption."[80] Where the cyber threat constitutes a material risk, the company should describe the type and severity of the risk, and should "avoid generic 'boilerplate' disclosure."[81] In some cases, that may require the disclosure of actual known or threatened cyber incidents.[82]

The Corp Fin Division's disclosure guidance also provides that if the costs or other consequences related to actual or potential cyber breaches "represent a material event, trend, or uncertainty," they should be addressed in a public company's MD&A section.[83] This too may require the disclosure of actual cyber incidents where, for example, the resulting costs are likely to be material or have led to a material increase in cybersecurity spending.[84] Since the SEC's disclosure guidance was first issued, the Corp Fin Division has issued a number of comment letters to public companies regarding their cybersecurity disclosures,[85] and speculation has emerged that the SEC is considering regulations requiring more specific disclosures surrounding cyber incidents.[86]

SEC Guidance for Registered Entities

Aside from the Corp Fin Division's disclosure guidance for public companies, the SEC addressed cybersecurity for regulated entities through the Division of Investment Management (the "IM Division"), which regulates investment companies, variable insurance products, and federally registered investment advisers,[87] and the Office of Compliance Inspections and Examinations ("OCIE"), which "administer[s] the SEC's nationwide examination and inspection program" for registered entities, including broker-dealers, transfer agents, investment advisers, investment companies, the national securities exchanges, and clearing agencies.[88]

The IM Division issued cybersecurity guidance that outlined steps for registered investment companies and registered investment advisers to consider.[89] The guidance recommends that these registered entities conduct periodic assessments; develop a strategy that is designed to prevent, detect, and respond to cybersecurity threats—including instituting preventative security measures and creating an incident response plan; and implement the strategy through written policies and procedures and training. [90] The guidance also recommends that funds and advisers assess the cybersecurity measures in place at relevant third-party service providers.[91]

On the examination front, OCIE announced the launch of a Cybersecurity Examination Initiative by issuing a Risk Alert in April 2014.[92] The 2014 Risk Alert offered a useful roadmap for the types of questions firms can expect to face during an examination. The Alert included, for example, a sample exam letter requesting information about past cyber incidents, cybersecurity governance, protection of firm networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and methodology for identifying best practices.[93]

About 10 months later, in February 2015, OCIE released a follow-up Risk Alert providing summary observations from its examinations of 57 registered broker-dealers and 49 registered investment advisers conducted under the 2014 Initiative.[94] The 2015 Risk Alert provides data points from the OCIE's examinations that can be used to inform cybersecurity policies and practices.

For example, OCIE found a gap, particularly among investment advisers, when it comes to the level of scrutiny applied to cybersecurity at third-party vendors. While most of the examined firms performed risk assessments on a firm-wide basis, only 32% of the advisers required cybersecurity assessments of vendors with access to their networks, and even fewer (24%) incorporated requirements relating to cybersecurity risk into their contracts with vendors and business partners.[95] As cybercriminals have increasingly looked to exploit vulnerabilities at third-party vendors as a backdoor into companies' networks, companies should not overlook the need to apply the same type of rigor to outside vendors that they do to their own networks.[96] Efforts to fortify internal defenses are wasted if attackers can simply achieve the same result by taking advantage of weaknesses in cybersecurity at third-parties.

The 2015 Risk Alert also reported that over half of the examined broker-dealers (54%) and just under half of the examined advisers (43%) had received fraudulent emails seeking to transfer client funds.[97] A number of firms that experienced losses as a result of such fraudulent emails said that those losses were the result of employees not following identity authentication procedures.[98] These findings further highlight the importance of employee education and training as part of an effective cybersecurity program.

In September 2015, OCIE issued a new Risk Alert outlining the areas on which OCIE intends to focus in its second round of cybersecurity examinations, a process "which will involve more testing to assess implementation of firm procedures and controls."[99] The areas include governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.[100]

SEC Rulemaking and Enforcement Activity

The SEC also has implemented rules that relate directly or indirectly to cybersecurity and have been—and likely will increasingly be—the basis for enforcement actions. The principal such regulation is Rule 30 of Regulation S-P (referred to as the "Safeguard Rule"), which requires that brokers, dealers, investment companies, and registered investment advisors develop and implement written policies and procedures reasonably designed to "(a) [i]nsure the security and confidentiality of customer records and information; (b) [p]rotect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) [p]rotect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[101] The Safeguard Rule has been the basis for enforcement actions against firms and individual executives for cybersecurity deficiencies,[102] and can be expected to serve as the basis for future enforcement actions as regulatory scrutiny of cybersecurity practices increases.

In fact, just last week, the SEC relied to the Safeguard Rule to deliver on its earlier statement that cybersecurity is an area "high on [the SEC's] radar screen."[103] The SEC announced charges against a St. Louis-based investment adviser that, according to the SEC, had "failed to establish the required cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients."[104] The SEC expressly acknowledged that no evidence existed of financial harm to any of the firm's clients, but determined that enforcement proceedings were nevertheless appropriate in light of the "increasing barrage of cyber attacks on financial firms."[105] Among the firm's alleged failures were that it "failed to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server, or maintain a response plan for cybersecurity incidents."[106]

In addition, in November 2014, the SEC adopted Regulation Systems Compliance and Integrity ("Regulation SCI"), which requires certain key market participants, including registered national securities exchanges and clearing agencies, to take steps designed to reduce the occurrence of data breaches and improve resiliency in the event of a breach.[107] Regulation SCI provides a framework for these entities to implement policies and procedures to help ensure operational capability, take appropriate corrective action when systems issues occur, provide notifications and reports to the SEC regarding systems problems and systems changes, inform members and participants about systems issues, conduct business continuity testing, and conduct annual reviews of their automated systems.[108]

Financial Industry Regulatory Authority

The SEC has not been the only source of guidance for broker-dealers. Earlier this year, FINRA issued detailed guidance to address the threat of a cyber incident.[109] FINRA's guidance provides specific recommendations for ensuring each of the following: risk assessments, a governance framework, technical controls and preventative measures, incident response plans, training of employees, and intelligence sharing. Like the SEC, FINRA has relied on the Safeguard Rule to bring enforcement actions in the wake of a data breach. FINRA fined a regulated firm for failing to protect confidential customer information after international hackers obtained information regarding approximately 192,000 customers,[110] and recently entered into a settlement with another firm that faced an information security threat after an unencrypted laptop containing sensitive information about hundreds of thousands of clients was left unattended in a restroom.[111]

Federal Communications Commission

The FCC encourages communications companies to practice "proactive and accountable self-governance within mutually agreed parameters" with respect to cybersecurity, and facilitates the improvement of cyber-risk management and corporate accountability in the communications sector through the Communications Security, Reliability and Interoperability Council.[112] The FCC also has prioritized enforcement actions in cyber breach cases. In April of this year, the agency entered into a consent decree with AT&T after nearly 280,000 customers' personal data was compromised.[113] In what the FCC called the "largest privacy and data security enforcement action to date," AT&T agreed to pay a $25 million penalty, hire a senior compliance office, conduct a privacy risk assessment and adopt various other reforms.[114] Companies in the communications sector should expect the FCC to continue its enforcement attention on perceived cybersecurity lapses in the future.

Department of Health & Human Services

The Health Insurance Portability and Accountability Act ("HIPAA") Security Rule established "national standards for protecting the confidentiality, integrity, and availability of electronic protected health information," and HHS's Office of Civil Rights ("OCR") is charged with the administration and enforcement of HIPAA's Privacy and Security Rules.[115] In May 2014, two health care organizations entered into a settlement with the HHS OCR for $4.8 million after allegedly failing to adequately secure "thousands of patients' electronic protected health information" that was "held on their network," in the largest HIPAA settlement to date.[116]

Federal Trade Commission

The FTC has been particularly active in the area of cybersecurity, bringing over 50 civil actions against companies related to the protection of personal information, using its authority under the Gramm-Leach-Bliley Act ("GLBA"), Section 5 of the FTC Act (which prohibits unfair or deceptive practices), and the Fair

Credit Reporting Act.[117] The United States Court of Appeals for the Third Circuit recently upheld the FTC's authority to bring suits under Section 5 of the FTC Act based on "unfair or deceptive" cybersecurity practices.[118] The Third Circuit ruled that the alleged conduct—breaches of a hotel chain's data which resulted in over $10.6 million in fraudulent charges—did not "fall[] outside the plain meaning of 'unfair.'"[119] This decision may embolden the FTC to increasingly prioritize data security and privacy issues in its enforcement initiatives.

The FTC's relatively sweeping—and potentially expanding—authority to regulate cybersecurity issues is further evidenced by its issuance of the Health Breach Notification Rule in 2009, which requires certain businesses that are "not covered by HIPAA to notify their customers and others if there's a breach of unsecured, individually identifiable electronic health information."[120] The agency began enforcing the rule in February 2010.[121]

State Attorneys General

Forty-seven states, the District of Columbia, Puerto Rico, and the Virgin Islands have laws requiring notification of security breaches involving personal information, and a number of state attorneys general have been active in this area. About 15 state attorneys general, led by Illinois and Connecticut, are reportedly investigating a 2014 cyber breach at a major financial institution.[122] As lawmakers consider enacting federal legislation that sets nationwide guidelines for customer notification in the case of a data breach, the "[a]ttorney generals from all 47 states with data breach notification laws are urging Congress not to preempt local rules with a federal standard," arguing that the states currently play an "important role" in protecting consumers from cyberattacks.[123]

Federal Bank Regulators

The federal bank regulators—the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA")—have responsibility for ensuring the safety and soundness of the institutions they oversee, protecting federal deposit insurance funds, promoting stability in financial markets, and enforcing compliance with applicable consumer protection laws. These regulators individually and collectively have prioritized cybersecurity and have been working with industry and interagency organizations to improve financial institution cybersecurity.

Financial Stability Oversight Council

The Financial Stability Oversight Council ("FSOC"), established by the Dodd-Frank Act to "identify risks to the [country's] financial stability," "promote market discipline," and "respond to emerging threats to the stability of the U.S. financial system," has addressed the issue of cybersecurity.[124] Earlier this year, FSOC—whose members include the heads of each of the bank regulators—released its annual report, in which it identified cybersecurity as requiring "heightened risk management and supervisory attention."

The report warned that "recent cyber attacks have heightened concerns about the potential of an even more destructive incident that could significantly disrupt the workings of the financial system."[125] The FSOC advised that "[m]itigating risks to the financial system posed by malicious cyber activities requires strong collaboration among financial services companies, agencies, and regulators."[126]

Individual Bank Regulators

Each of the individual bank regulators have also emphasized the importance of cybersecurity. In its Spring 2015 Semiannual Risk Perspective, for example, the OCC identified cybersecurity as one of its top supervisory concerns, and a priority for the next twelve months.[127] The report noted that, consistent with guidance from the other regulators, the OCC's bank examinations "will include assessments of data and network protection practices, business continuity practices, risks from vendors, and compliance with any new guidance."[128] A senior representative of the Federal Reserve Bank of New York emphasized that "cybersecurity is a 'new normal.' It is going to become part of our vocabulary in nearly every exam we conduct, conversation we have with senior management, and conversation about the future of financial services."[129] Benjamin Lawsky, who recently stepped down as the Superintendent of the New York Department of Financial Services, called cybercrime "a huge threat to our financial system" and predicted that there would be "a lot of action around cybersecurity and the regulation in that area."[130]

Federal Financial Institutions Examination Council

The banking regulators have collaborated and coordinated on cybersecurity through the FFIEC, a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions and to make recommendations to promote uniformity in the supervision of financial institutions. Two key forms of guidance issued by the FFIEC are the Information Technology Examination Handbook and the Cybersecurity Assessment Tool, which was released this summer and discussed in detail below.

The FFIEC's IT Examination Handbook, first published in 1980, "comprises 11 booklets addressing topics such as electronic banking, information security, and outsourcing technology services."[131] FFIEC has updated the Handbook, and the FFIEC and individual regulators have issued guidance to address particular threats facing the industry, such as DDoS attacks, account takeovers, advanced persistent threats, and credit/debit card breaches.[132] There are now more than 150 examples of cybersecurity guidance applicable to the banking and finance sector.[133]

Gramm-Leach-Bliley Act

Financial institutions also are subject to certain regulations and interagency guidance issued pursuant to the GLBA. Section 501(b) of GLBA mandated that the bank regulators issue information security standards for financial institutions to safeguard sensitive customer information. Member agencies of the FFIEC did so by issuing the Interagency Guidelines Establishing Information Security Standards (the

"Security Guidelines"). Under the Security Guidelines, each financial institution must develop and maintain an effective information security program tailored to the complexity of its operations, and service providers that have access to its customer information are required to take appropriate steps to protect the security and confidentiality of this information.[134] The Security Guidelines require each financial institution to identify and evaluate risks to its customer information, develop a plan to mitigate the risks, implement the plan, test the plan, and update the plan when necessary. Each financial institution must also report to its board "at least annually" on its information security program and compliance with the Security Guidelines.[135] The standards set forth in the Security Guidelines are consistent with the IT Examination Handbook and other guidance from the FFIEC member agencies. The Security Guidelines afford the FFIEC agencies enforcement options if financial institutions do not establish and maintain adequate information security programs.[136]

Pursuant to its authority under the GLBA, the FTC issued the Safeguards Rule, requiring certain non-bank financial institutions under the FTC's jurisdiction to have an information security plan that "contains administrative, technical, and physical safeguards" to "insure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."[137]

Financial institutions should endeavor to follow regulatory guidance to ensure best practices in cybersecurity and to mitigate their regulatory risk. In addition, being responsive to this guidance is essential because private plaintiffs are likely to rely on any deviation from the regulatory guidelines as purported evidence of inadequate cybersecurity in the wake of a cyber incident. In one case, for example, the United States Court of Appeals for the First Circuit determined that a bank's security procedures were not "commercially reasonable" based in part on the bank's failure to adhere to FFIEC guidance.[138]

Best Practices for Boards and Senior Management

The frequency and scope of recent cyberattacks and the corresponding increased costs and harm demonstrate that the cyber threat is one of the most significant business risks facing financial institutions and other businesses. As a result, cybersecurity is a governance issue that requires attention from directors and senior leadership. In a recent study, "79 percent of C-level US and UK executives surveyed sa[id] executive level involvement is necessary to achiev[e] an effective incident response to a data breach and 70 percent believed board level oversight is critical."[139] Below is a summary of some of the key practices for boards and senior management to consider.

Board Oversight

As one SEC Commissioner stated, "ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's [*sic*] risk oversight responsibilities."[140] Senior management and

the board should consider whether a committee of the board (such as the Audit Committee or a Risk Committee) or the full board should have primary oversight responsibility for cybersecurity. In any case, the board should be briefed regularly about cyber risks and efforts to address and mitigate those risks. External advisers, including those with the requisite technical expertise, can be enlisted as necessary to help directors understand the risks and a company's preparedness to respond to those risks. The board should also consider whether particular members of management should be tasked with overseeing cybersecurity and reporting to the board on cybersecurity matters.

The National Association of Corporate Directors ("NACD") addressed the role of boards relating to cybersecurity and identified the following five principles: (1) "[d]irectors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue;" (2) "[d]irectors should understand the legal implication of cyber risks as they relate to their company's specific circumstances;" (3) "[b]oards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given adequate time on the board meeting agenda on a regular basis;" (4) "[d]irectors should set an expectation that management establish an enterprise-wide cyber-risk management framework with adequate staffing and budget;" and (5) "[b]oard-management discussion of cyber risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach."[141]

For financial institutions, the recently-released FFIEC Assessment Tool (discussed in detail below) provides a useful mechanism to evaluate the alignment between an institution's inherent risks and its cybersecurity preparedness. The FFIEC also released an overview for CEOs and directors along with the Assessment Tool that, among other things, lists questions for management and directors to consider and guide their discussions when using the Assessment Tool.[142] Although a valuable resource, the Assessment Tool "is intended to complement, not replace, an institution's risk management process and cybersecurity program."[143]

Periodic Risk Assessments

Periodic risk assessments should be conducted to develop a meaningful understanding of the key cyber risks facing the organization. It is impossible to design a program tailored to a particular company's risks and operations without first understanding those risks and how they impact the company's business. Accordingly, the board and senior leadership should be briefed regularly on the institution's cyber risks and the measures in place to mitigate those risks. The risk assessments should identify the company's most sensitive and valuable information and assets, and the company's senior leadership should understand where and how that information is stored, and the ways in which it is protected. Those assets should be afforded the greatest level of security protection.

Preventative Measures: Technology, Controls and Compliance

The board and senior management should ensure that the company has implemented sufficient preventative measures and controls and that they are being periodically reviewed and updated as necessary. Technology is, of course, a critical component of defending against a cyberattack, and companies should follow the best practices outlined in the applicable regulatory guidelines. Technological measures, however, cannot be relied on exclusively. Employees remain a significant source of potential vulnerability that cybercriminals continue to exploit, and therefore, an effective cybersecurity program must incorporate employee training and education and information-security controls. Notwithstanding the risk from insiders, this aspect of cybersecurity is often neglected. In one survey, for example, only 50 percent of respondents said they conduct periodic security awareness and training programs, and the same number said they offer security training for new employees.[144]

Although many companies have developed robust compliance programs in areas ranging from anti-bribery to anti-money laundering to insider trading, compliance efforts on the information-security side are often lagging, even though the risk to the overall organization from non-compliance by a single employee may be potentially greater in the cyber area. New hires and existing personnel should all be trained on the importance of cybersecurity, educated as to the risks and their individual roles in protecting the company against those risks, and advised of the company's information-security policies. Compliance with information-security policies should be monitored, just as employees' compliance with securities trading or other more traditional areas of compliance are routinely monitored.

Employee training should be provided periodically and updated as necessary, and employees should be required to sign regular cyber-compliance certifications. The importance of information security needs to be emphasized, and the message should come from the top of the organization to instill a strong culture of information security throughout the organization. Basic policies and protocols that reduce risks should include requiring encryption, limiting the use of personal devices, using strong passwords that must be changed periodically, and controlling remote access through multifactor authentication.

Taking these steps to enhance cybersecurity can present a difficult balance for companies because each enhanced security measure typically imposes an additional burden on employees. It could become convenient for employees to bypass these measures, so it is critically important that information-security policies be prioritized, and that the proper tone is set by management. Further, there are effective measures that impose a relatively low burden and yet, surprisingly, still are not implemented by many sophisticated organizations until after they are victimized. In the wake of the OPM hack, for example, the White House announced a "Cybersecurity Sprint" designed to improve cybersecurity at federal agencies over a 30-day period, and that effort has included basic measures that had not been widely implemented. As one example, in just the first 10 days of the Sprint, federal civilian agencies reportedly were able to increase multifactor authentication—an effective and not burdensome measure—by 20 percent.[145]

Moreover, given the increased awareness of the severity of the risk among the general public, there is reason to be optimistic that employees will have at least a modestly increased tolerance for some additional burdens in order to fortify their companies' cybersecurity.[146]

As the nature of the cybersecurity threat evolves, and additional risks or vulnerabilities are identified, cybersecurity policies and protocols must be updated accordingly. For example, the need for increased oversight and scrutiny of third-party vendor relationships has become evident as cybercriminals have increasingly exploited weaknesses in vendor security to bypass a company's cybersecurity. The Target breach is perhaps the most high-profile example, but the DOJ's recent announcement of a massive insider trading ring that relied on the hacking of business newswires further highlights the risks associated with providing network access or sensitive data to third-party vendors. Management should require appropriate vendor management controls, including diligence, monitoring and contractual protections.

Information Sharing with Government and Industry Peers

A comprehensive cybersecurity program should include a mechanism for sharing information with public and private partners to enhance access to actionable cyber-threat intelligence that can be used to better detect and respond to threats. As discussed below in the context of the GAO Report, the financial sector is among the leaders in this effort. Although lawmakers and regulators are exploring ways to improve cyber information sharing, institutions must continue working collaboratively to remove barriers to more robust sharing and to find innovative ways to enhance the effectiveness of their information sharing. Information sharing is also an important tool for smaller institutions, which tend to have less sophisticated defense mechanisms and fewer IT resources; by helping them focus their limited resources, cyber-threat intelligence can be particularly important to those institutions.

Review and Satisfaction of Applicable Legal and Regulatory Requirements

The legal and regulatory framework governing cybersecurity is fragmented and evolving. Companies must navigate a maze of domestic and international cyber-related laws and regulations that apply in both the pre-breach and post-breach context. Companies have legal, regulatory and often contractual obligations to safeguard information and, following a breach, to make certain disclosures to customers, regulators, or other third-parties. In the post-breach context, for example, 47 states, the District of Columbia, Puerto Rico, and the Virgin Islands have laws requiring notification of security breaches involving personal information, and industry-specific laws and regulations impose independent notification obligations. As discussed above, public companies also have public disclosure obligations, and SEC-regulated entities are subject to separate SEC regulations concerning the safeguarding of information. Senior leadership should understand not only the business risks associated with the cyber threat but also the legal and regulatory risks and requirements. Management should ensure ongoing compliance with those requirements and, as discussed below, oversee the company's preparedness to satisfy its legal, regulatory, and contractual obligations in the event of a breach. Just as advance planning can mitigate the business risks, it can also mitigate the legal and regulatory exposure from a cyberattack.

Incident Response and Business Continuity Plan

Because no defense system is impenetrable, it is critical not only to ensure adequate preventative measures, but to have a comprehensive incident response and business continuity plan that can quickly be implemented in the event of a breach. In the wake of an attack, companies face a host of challenges and must make difficult and time-sensitive decisions, typically with incomplete information and in a chaotic environment. The way in which companies respond can directly impact the extent of the resulting harm, including financial loss, reputational harm, and civil and regulatory liability—all of which can be mitigated through advance planning and maximum preparedness.

Some of the key issues that typically arise following a breach are: (1) assessing the scope of the attack, determining what, if anything, has been taken, and ensuring that any intruders are completely removed from the network. This is a process that is usually far more difficult and time-consuming than most organizations anticipate, which further compounds the challenge of responding to an attack because the scope of the breach typically cannot be determined quickly, meaning that companies will have to make difficult decisions despite lacking key facts and critical information; (2) quickly restoring and ensuring continuity of business operations with minimal disruption, even in the case of destructive malware; (3) complying with domestic and international statutory and regulatory disclosure requirements, and determining when and to whom disclosures should be made, as well as what should be disclosed; (4) deciding if and when to notify law enforcement authorities and, if so, dealing with the day-to-day interactions with those authorities as they conduct investigations; and (5) handling internal communications and external public relations with consumers, shareholders and other affected third-parties.

Given the range of issues that arise, a comprehensive response requires an integrated approach involving the participation not only of senior leadership but of representatives from a number of different internal constituencies, such as IT, legal, compliance, and investor relations, as well as outside technical, legal, and PR advisors. Companies should not put themselves in the position of confronting these difficult questions for the first time, or scrambling to determine who should be responsible for what, in the chaotic aftermath of a cyber incident. Companies need to consider each of these issues in advance of an attack. The response plan should provide clearly delineated lines of responsibility for each of the significant issues likely to arise following a breach and should be tested through tabletop exercises before an incident occurs.

The risk of a cyberattack cannot be eliminated. But the impact can be mitigated through careful planning, and it is therefore essential that boards and senior leadership take the steps necessary to put their companies in the best position to limit the resulting harm should an incident take place.

Recent Developments Affecting Financial Institutions

Recognizing the unique threats facing the industry, the GAO and FFIEC each released cybersecurity resources this summer specifically tailored to financial institutions. We examine both the GAO Report and the FFIEC Cybersecurity Assessment Tool in detail below.

The GAO Report on Cybersecurity at Banks and Other Depository Institutions

In July of this year, the GAO released a report on cybersecurity at banks and other depository institutions.[147] The report principally examined (1) how bank regulators oversee depository institutions' efforts to mitigate cyber threats, and (2) how government agencies share cyber threat information with the banking sector. The report's key conclusions were: first, while bank regulators focus their cybersecurity examinations on risks *within* individual institutions, the regulators need to collect and analyze data from IT examinations on trends *across* the industry; and second, notwithstanding fairly robust sharing of cyber-threat information among financial institutions, obstacles still remain, and banks are seeking more usable threat information from their government counterparts.

Bank regulators take an institutional, risk-based approach to their cybersecurity examinations. Accordingly, the scope of an IT examination at any particular institution is determined based on an assessment of that institution's internal and external risks. To assess those risks, examiners look at an institution's safeguards and protections against threats to customer information, the likelihood and effects of identified threats and vulnerabilities, and the sufficiency of policies and procedures to control risks.

Hiring and training a sufficient number of examiners with the requisite expertise to conduct sophisticated examinations poses a serious challenge for regulators. To put the problem in perspective, the FDIC is the primary regulator for over 4,000 institutions, and has only "60 premium IT examiners who are highly skilled in conducting IT examinations;" the OCC is the primary regulator for more than 1,500 institutions, and has "100 dedicated IT specialist examiners;" the NCUA "regulates more than 6,200 credit unions" and has "40 to 50 subject-matter IT examiners" and 16 IT specialists; and the Federal Reserve "regulates more than 5,500 institutions" and has approximately 85 IT examiners with information security or advanced IT expertise.[148]

Faced with these resource constraints, regulators generally have not used IT experts for examinations of medium and small institutions, meaning that "examiners with little or no IT expertise are performing IT examinations at smaller institutions."[149] This allocation of limited resources is understandable, but concerning, especially given that the discrepancy in sophistication of examiners parallels the disparity in information-security resources across such institutions. Smaller institutions, not surprisingly, tend to devote fewer resources to information security. One large bank said it planned to deploy over 1,000 people to focus on cybersecurity,[150] and following a significant breach last year, that bank's CEO

announced that the bank would double its $250 million annual spending on cybersecurity.[151] By contrast, some community banks do not have any dedicated IT security personnel.[152] This may leave smaller financial institutions more vulnerable to cyberattacks, perhaps explaining why cybercriminals appear increasingly to be targeting smaller financial institutions.[153]

The principal deficiency identified in the GAO Report, however, was the failure of regulators to aggregate data from individual examinations to identify trends across the industry: "Although each regulator described collecting some information across examinations to assist its oversight, the regulators did not have standardized methods for collecting examination data that could allow them to readily analyze trends in specific information security problems across institutions."[154]

The failure stems in part from the methods by which regulators collect information from individual institutions. In particular, the information is not collected in formats that would facilitate such aggregation and analysis. The regulators, for example, do not have standardized methods for categorizing IT deficiencies. The deficiencies identified at particular institutions generally were not broken into fields or categories that differentiated the types of problems found at different institutions, and thus the regulators are not able to identify trends in specific types of deficiencies across institutions. In addition, although banks have obligations to disclose to their regulators data breaches that compromise sensitive customer information, the information collected by the regulators is not centrally compiled and analyzed. The GAO found that the regulators "varied in the extent to which they could provide data on actual incidents at their regulated institutions."[155]

The GAO Report concluded that these flaws have hindered the regulators from identifying broader IT issues affecting their regulated entities and thus impede their ability to better target their IT risk assessments. This is not the first time—and cybersecurity is not the first area—in which the GAO has observed this deficiency in how regulators collect and analyze information. In a January 2000 report, the GAO observed "that neither the Federal Reserve nor OCC collected aggregated information on the risks that examiners identified during examinations."[156] As an example of the potential benefits of such an approach, the January 2000 report concluded that by aggregating examination data, regulators would have been better positioned to recognize the industry-wide exposure to Long Term Capital Management and appreciate the potential disruption to the markets of its collapse.[157] And in 2009, the GAO "found that bank regulators' oversight of institutions' anti-money laundering activities could be improved by aggregating information about deficiencies."[158]

The second key conclusion of the GAO Report was that improvements are needed in the way cyber-threat information is shared among the financial sector and disseminated from the government to the private sector. While the government has been engaged in a campaign to encourage the private sector to share more information with the government, the GAO Report identifies deficiencies in the flow of information *from* the government *to* the private sector.

The financial industry has developed sophisticated information-sharing mechanisms and established a model that other industries have sought to emulate. The Financial Services Information Sharing and Analysis Center ("FS-ISAC"), for example, has become a key resource for cyber-threat information for financial sector institutions. The FS-ISAC was established in 1999 and is the operational arm of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security ("FSSCC"). The FS-ISAC facilitates the sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures and practices. It has over 5,000 members worldwide, and when it learns of an attack or has other information to share, it follows a protocol in which different color-coded alerts indicate who can access the information.[159] During the OCIE examination sweep, broker-dealers identified the FS-ISAC as "adding significant value,"[160] and banks have reported that a high level of trust has developed among the FS-ISAC members and that the FS-ISAC was valuable in responding to the financial-sector DDoS attacks.[161] The DDoS attacks showcased the "sector's capacity . . . , through the FS-ISAC, [to] act collectively to respond to major attacks and minimize their capacity to cascade through the sector."[162]

The financial sector has also developed and implemented innovations to facilitate more robust information sharing. For example, to help alleviate concerns about exposing competitive weaknesses by revealing breaches to competitor institutions, the FS-ISAC removes identifying data to obscure the identity of the breached institution.[163] Although some reluctance to share information for this reason remains, this approach has reduced the concern. The FS-ISAC has also deployed an automated system called Soltra Edge, which was developed in conjunction with DHS, the Depositary Trust, and Clearing Corporation, for efficiently disseminating alerts to member institutions.[164]

The government is also an important source of cyber threat information for financial institutions. In nearly 70 percent of all breaches, organizations first learn of the breach from the government or some other external source.[165] The primary government sources of cyber information for the financial sector are Treasury, DHS, Secret Service, and the FBI. Treasury's Financial Sector Cyber Intelligence Group ("CIG"), for example, monitors and analyzes intelligence on cyber threats to the financial sector and disseminates that information to industry participants. The CIG facilitates the sharing of classified information and also responds to requests for information from financial institutions, either individually or through the FS-ISAC. Law enforcement agencies, like the FBI Cyber Division and the Secret Service's Electronic Crimes Task Forces, often share threat information directly with financial institutions or through the use of Private Industry Notification Reports addressing particular threats. And representatives of financial institutions are often provided temporary security clearances so they can receive threat briefings from the FBI or other agencies.

Although the financial industry has developed extensive information-sharing arrangements both within the private sector and between the private sector and government, the GAO Report identifies obstacles that remain and offers suggestions for improvements to the way in which the government disseminates

information to the industry. In particular, financial institutions have expressed frustration that the information they receive is often "repetitive," "not timely," and "lack[ing] sufficient details" to be actionable.[166]

By virtue of having multiple sources of information within government, banks often end up receiving the same information from multiple agencies.[167] That redundancy causes banks to waste resources trying to determine whether the information is new or duplicative. While this creates an unnecessary distraction of IT resources for banks of all sizes, it poses an even greater challenge for smaller institutions that are already grappling with limited information-security resources.

Banks also reported that for the information to be effective, it must be timely and specific.[168] The timeliness of information sharing can be critical in effectively defending against a cyberattack that quickly spreads from one institution to another. One report found that 75 percent of cyberattacks spread from victim 0 to victim 1 within 24 hours, and "[o]ver 40% hit the second organization in less than an hour."[169] As to the specificity of the information, the GAO Report determined that the information banks obtain from the government often lacks context or specific details necessary to enable banks to take steps to protect themselves. A representative of a financial institution offered this analogy: "receiving insufficiently detailed information [is] similar to telling the institution that it might be attacked by a criminal in a red hat. But saying that a criminal in a red hat, would go behind the building, and use a crowbar to force the door open would provide enough detail for the institution to better target its defenses."[170]

The government is already taking steps to reduce obstacles to better information sharing. Treasury, for example, is seeking to accelerate the declassification of financial cyber threat information, which should enable the sharing of more specific information. Deputy Treasury Secretary Sarah Bloom Raskin recently said that Treasury is focused on "getting information declassified very quickly and into the hands of people who need it," adding, "It makes no sense for the government to be sitting on this information."[171]

While the GAO Report focused mainly on potential improvements in the flow of information from government to the private sector, it also identified issues that continue to restrict complete sharing in the other direction. There is, for example, continuing concern within the private sector about potential liability resulting from the sharing of personal information with the government, as well as fears that the information may become classified (which, in turn, restricts further sharing of the information by the institution) or subject to public disclosure (through FOIA requests, for example).[172]

Congress and the White House have been working to alleviate these concerns as well. In February, President Obama issued Executive Order 13,691 on Promoting Private Sector Cybersecurity Information Sharing, which directs the Secretary of Homeland Security to "strongly encourage" the development of Information Sharing and Analysis Organizations ("ISAOs") to serve as focal points for cybersecurity collaboration.[173] The President also proposed legislation that would protect companies from lawsuits for sharing certain cybersecurity information

with the government.[174] Two pending bills in the House and one in the Senate seek to provide private companies protection from liability in order to encourage sharing of information with the government.[175]

The FFIEC Cybersecurity Assessment Tool

This summer, the FFIEC rolled out a Cybersecurity Assessment Tool (the "Assessment Tool") to give financial institutions a "repeatable and measurable process to inform management of their institution's risks and cybersecurity preparedness."[176] The Assessment Tool incorporates principles from the IT Handbook and the National Institute of Standards and Technology ("NIST") Framework.

The Assessment Tool is broken down into two parts. The first addresses an institution's Inherent Risk Profile, and the second addresses the company's Cybersecurity Maturity. It enables an institution to evaluate its level of risk in each of five enumerated risk categories, and its level of cybersecurity preparedness in each of five "domains." By comparing the institution's risk levels to its cybersecurity maturity levels, management can assess whether the degree of maturity is sufficiently aligned with its level of risk. If not, the Assessment Tool provides readily identifiable measures the company can take to reduce a particular risk or increase the maturity of a particular aspect of its cybersecurity.

The Inherent Risk Profile assigns one of five escalating risk levels (least, minimal, moderate, significant, or most) to each of five categories of risk: (1) technologies and connection types, (2) delivery channels, (3) online/mobile products and technology services, (4) organizational characteristics, and (5) external threats. For each category, the Assessment Tool lists different parameters that correlate to each risk level. For example, within the "technologies and connection types" category, one of the considerations is the number of personal devices allowed to connect to the corporate network. The institution determines its risk level by choosing the parameters that best describe the company's characteristics. The following table provides an example of the characteristics, or parameters, corresponding to each of the risk categories for "personal devices":[177]

	Risk Level				
	Least Risk	Minimal Risk	Moderate Risk	Significant Risk	Most Risk
Personal devices allowed to connect to the corporate network	None	Only one device type available; <5% of employees; e-mail access only	Multiple device types used; available to <10% of employees; e-mail access only	Multiple device types used; available to <25% of authorized employees; e-mail and some applications	Any device type used; available to >25% of employees; all applications accessed

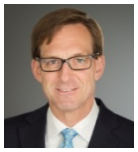
After determining the Inherent Risk Profile, the institution turns to the Cybersecurity Maturity portion of the Assessment Tool to determine its maturity level within each of five "domains:" (1) "Cyber Risk Management and Oversight," (2) "Threat Intelligence and Collaboration," (3) "Cybersecurity Controls," (4) "External Dependency Management," and (5) "Cyber Incident Management and Resilience."[178] Within each domain, the Assessment Tool lists declarative statements that apply to each maturity level (baseline, evolving, intermediate, advanced, or innovative). The institution determines its maturity level by identifying which declarative statements best fit the current practices of the company. The Assessment Tool thereby allows a company to determine its maturity level within each of the five domains, but does not provide an overall enterprise-wide maturity level.

When the assessment is complete, management can assess the degree of alignment between its risk profile and its cybersecurity maturity. An institution's maturity level generally should go up as its risk profile rises. Because the risk profile and maturity levels will change over time, the Assessment Tool recommends that management reevaluate both periodically and be vigilant of planned changes (like new products or services or new connections) that may affect its risk profile.

The Assessment Tool is a useful management oversight resource because it provides a method for comparing an institution's maturity level to its inherent risk profile. To the extent management is not satisfied with the level of maturity in relation to its risk profile, the characteristics of the different categories provide actionable steps that management can take either to reduce its risk level or to enhance its maturity level.

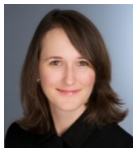
* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

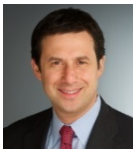


John F. Baughman
Partner
212-373-3021
jbaughman@paulweiss.com

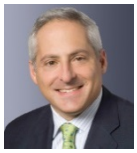
H. Christopher Boehning
Partner
212-373-3061
cboehning@paulweiss.com



Jessica Carey
Partner
212-373-3566
jcarey@paulweiss.com

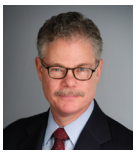


Roberto Finzi
Partner
212-373-3311
rfinzi@paulweiss.com



Michael E. Gertzman
Partner
212-373-3281
mgertzman@paulweiss.com

Brad S. Karp
Partner
212-373-3316
bkarp@paulweiss.com



Daniel J. Kramer
Partner
212-373-3020
dkramer@paulweiss.com

Lorin L. Reisner
Partner
212-373-3250
lreisner@paulweiss.com

Elizabeth M. Sacksteder
Partner
212-373-3505
esacksteder@paulweiss.com

Richard C. Tarlowe
Counsel
212-373-3035
rtarlowe@paulweiss.com

1 PwC, US Cybersecurity: Progress Stalled, Key Findings from the 2015 US State of Cybercrime Survey, PwC 3 (July 2015), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

2 *NYSE Tweets—"The Issue We Are Experiencing Is An Internal Technical Issue And Is Not The Result Of A Cyber Breach,"* CNBC (July 8, 2015, 12:28 PM), http://www.cnbc.com/2015/07/08/reuters-america-nyse-tweets--the-issue-we-are-experiencing-is-an-internal-technical-issue-and-is-not-the-result-of-a-cyber-breach.html.

3 Press Briefing, Press Secretary John Earnest, Press Secretary, Office of the Press Secretary, White House (July 8, 2015), https://www.whitehouse.gov/the-press-office/2015/07/08/press-briefing-press-secretary-josh-earnest-7815.

4 *The Latest: NYSE Trading Resumes After Outrage*, THE ASSOCIATED PRESS, (July 8, 2015, 3:59PM), http://bigstory.ap.org/article/131d63c2119340618b3ca160d546e4ce/latest-nyse-halts-trading-because-technical-issues.

5 *Jeh Johnson: United, NYSE Problems Not Caused By 'Nefarious' Actor*, REUTERS, (July 8, 2015), http://www.reuters.com/video/2015/07/08/jeh-johnson-united-nyse-problems-not-cau?videoId=364876319.

6 Press Release, U.S. Dep't of Justice, Nine People Charged in Largest Known Computer Hacking and Securities Fraud Scheme, (Aug. 11, 2015), http://www.justice.gov/usao-nj/pr/nine-people-charged-largest-known-computer-hacking-and-securities-fraud-scheme [hereinafter Press Release, Dep't of Justice].

7 Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach, (Sept. 22, 2015), http://www.sec.gov/news/pressrelease/2015-202.html.

8 Colleen McCain Nelson & Byron Tau, OPM Director Katherine Archuleta Resigns After Massive Personnel Data Breach, Wall St. J., http://www.wsj.com/articles/opm-director-katherine-archuleta-resigns-after-massive-personnel-data-hack-1436547193 (last updated July 10, 2015, 7:10 PM).

9 Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway—With Me in It, Wired, (July 21, 2015), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway; David Gelles, Hiroko Tabuchi, and Matthew Dolan, Complex Car Software Becomes the Weak Spot Under the Hood, N.Y. Times, (Sept. 27, 2015), http://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html.

10 Mike Spector & Danny Yadron, Regulators Investigating Fiat Chrysler Cybersecurity Recall, Wall St. J., http://www.wsj.com/articles/fiat-chrysler-recalls-1-4-million-vehicles-amid-hacking-concerns-1437751526 (last updated July 24, 2014, 8:37 PM).

11 Damien Paletta, FBI Director Sees Increasing Terrorist Interest in Cyberattacks Against U.S., Wall St. J., (July 22, 2015, 10:41 PM), http://www.wsj.com/articles/fbi-director-sees-increasing-terrorist-interest-in-cyberattacks-against-u-s-1437619297.

12 Ian McKendry & Tanaya Macheel, Regulators to Step Up Cybersecurity Activity: Lawsky, American Banker, (July 28, 2015), http://www.americanbanker.com/news/bank-technology/regulators-to-step-up-cybersecurity-activity-lawsky-1075715-1.html.

13 Michael Riley & Jordan Robertson, *Digital Misfits Link JPMorgan Hack to Pump-and-Dump Fraud*, BLOOMBERG BUSINESS, (July 21, 2015, 1:50 PM), http://www.bloomberg.com/news/articles/2015-07-21/fbi-israel-make-securities-fraud-arrests-tied-to-jpmorgan-hack (last updated July 22, 2015, 8:09 AM); Matthew Goldstein, *4 Arrested in Schemes Said to be Tied to JPMorgan Chase Breach*, N.Y. TIMES, (July 21, 2015), http://www.nytimes.com/2015/07/22/business/dealbook/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html.

14 James R. Clapper, Dir. of Nat'l Intelligence, S. Armed Forces Comm., Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community 1 (Feb.26, 2015), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf [hereinafter Clapper, Worldwide Threat Assessment].
15 *Id*.
16 IBM, IBM 2015 Cyber Security Intelligence Index: Analysis of Cyber Attacks and Incident Data from IBM's Worldwide Security Services Operations, app. at 3 fig.2 (2015), http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.PDF [hereinafter IBM 2015 Cyber Security Intelligence Index].
17 Verizon, 2015 Data Breach Investigations Report, 3 (2015), *available at* http://www.verizonenterprise.com/DBIR/2015 [hereinafter Verizon, 2015 Data Breach Investigations Report].
18 Mandiant, M-Trends 2015: A View From The Front Lines, FireEye 2 (2014), https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf [hereinafter Mandiant, A View From The Front Lines].
19 Worldwide Threat Assessment, *supra* note 14, at 2; see U.S. Gov't Accountability Office, GAO-15-509, Cybersecurity: Bank and Other Depository Regulators need Better Data Analytics and Depository Institutions Want More Usable Threat Information, at 9-11 (July 2, 2015), *available at* http://www.gao.gov/products/GAO-15-509 [hereinafter GAO-15-509].
20 GAO-15-509, *supra* note 19, at 13.
21 Press Release, Dep't of Justice, *supra* note 6.
22 Barry Vengerik et al., Hacking the Street? Fin4 Likely Playing the Market, FireEye (2014), https://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf.
23 Paletta, *supra* note 11.
24 See Mandiant, A View From The Front Lines, *supra* note 18, at 20-21; PwC, US Cybersecurity, *supra* note 1, at 4.
25 Worldwide Threat Assessment, *supra* note 14, at 1; see also Cyber Crime: Modernizing our Legal Framework for the Information Age: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary (July 8, 2015) [hereinafter Testimony of Wm. Douglas Johnson], *available at* http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Johnson%20Testimony.pdf (testimony of Wm. Douglas Johnson, American Bankers Association) ("Nation states are becoming more adept at compromising private and public computer systems for reasons ranging from retribution for perceived wrongs to espionage.").
26 Press Release, Fed. Bureau of Investigation, Update on Sony Investigation, (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.
27 Mark Mazzetti & David E. Sanger, U.S. Fears Data Stolen by Chinese Hacker Could Identify Spies, N.Y. Times, (July 24, 2015), http://www.nytimes.com/2015/07/25/world/asia/us-fears-data-stolen-by-chinese-hacker-could-identify-spies.html?_r=0.
28 Nicole Perlroth, Hackers in China Attacked The Times for Last 4 Months, N.Y. Times, (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.
29 David E. Sanger, Julie Hirschfeld Davis, & Nicole Perlroth, U.S. Was Warned of System Open to Cyberattacks, N.Y. Times, (June 5, 2015), http://www.nytimes.com/2015/06/06/us/chinese-hackers-may-be-behind-anthem-premera-attacks.html.
30 Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014),

http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
31 *Id.* (quoting Holder).
32 Worldwide Threat Assessment, *supra* note 14, at 2.
33 GAO-15-509, *supra* note 19, at 11.
34 *Id.*
35 Nicole Perlroth & Quentin Hardy, Bank Hacking Was the Work of Iranians, Officials Say, N.Y. Times, (Jan. 8, 2013), http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html; see also Worldwide Threat Assessment, *supra* note 14, at 3.
36 GAO-15-509, *supra* note 19, at 11, 13.
37 JPMorgan Chase & Co., Current Report (Form 8-K) (Oct. 2, 2014) at 2, *available at* http://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm.
38 *Id.*
39 Riley & Robertson, *supra* note 13; Goldstein, *supra* note 13.
40 Robin Sidel, Home Depot's 56 Million Card Breach Bigger Than Target's, Wall St. J., http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571 (last updated Sept. 18, 2014, 5:43 PM).
41 GAO-15-509, *supra* note 19, at 11-12.
42 *Id.*
43 Charles Riley, Insurance Giant Anthem Hit By Massive Data Breach, CNNMoney (Feb. 6, 2015, 10:52 AM), http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security.
44 Indictment, United States v. Turchynov, No. 2:15-cr-390 (D.N.J. Aug. 6, 2015), ECF No. 1; Indictment, United States v. Korchevsky, No. 1:15-cr-381 (E.D.N.Y. Aug. 5, 2015).
45 Press Release, U.S. Dep't of Just., Manhattan U.S. Attorney and FBI Assistant Director-In-Charge Announce Charges In Connection with Blackshades Malicious Software That Enabled Users Around The World to Secretly And Remotely Control Victims' Computers (May 19, 2014), http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection.
46 IBM 2015 Cyber Security Intelligence Index, *supra* note 16, at 6; Verizon Data Breach Investigations Report, *supra* note17, at 47.
47 IBM 2015 Cyber Security Intelligence Index, *supra* note 16.
48 Verizon Data Breach Investigations Report, *supra* note 17, at 13.
49 Target, Quarterly Report (Form 10-Q) (May 2, 2015) at 10, *available at* https://www.sec.gov/Archives/edgar/data/27419/000002741915000018/tgt-20150502x10xq.htm.
50 Dan Kaplan, Sony Expects to Spend at Least $171 million Over Breach, SC Mag., (May 23, 2011), http://www.scmagazine.com/sony-expects-to-spend-at-least-171-million-over-breach/article/203591.
51 Annie Lowrey, Sony's Very, Very Expensive Hack, N.Y. Mag., (Dec. 16, 2014, 5:47 PM), http://nymag.com/daily/intelligencer/2014/12/sonys-very-very-expensive-hack.html
52 Michael Cieply & Brooks Barnes, Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm, N.Y. Times, (Dec. 30, 2014), http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.
53 Complaint at 85-86, In re Target Corporation Consumer Data Security Breach Litigation, MDL No. 14-2522 (D. Minn. Aug. 25, 2014), ECF No. 182.
54 *Id.* at 1.

55 George Stahl, Target to Pay $10 Million in Class Action Over Data Breach, Wall St. J., (Mar. 19, 2015, 8:38 am), http://www.wsj.com/articles/target-to-pay-10-million-in-class-action-over-data-breach-1426768681.
56 *Id.*
57 Lisa Beilfuss, Target Reaches $19 Million Settlement with MasterCard Over Data Breach, Wall St. J., (Apr. 15, 2015, 6:17 PM), http://www.wsj.com/articles/target-reaches-19-million-settlement-with-mastercard-over-data-breach-1429136237.
58 Tina Orem, Target/MasterCard Settlement Deal Dead, Credit Union Times, (May 21, 2015), http://www.cutimes.com/2015/05/21/target-mastercard-settlement-deal-dead.
59 Shannon Pettypiece & Elizabeth Dexheimer, Target Reaches $67 Million Agreement with Visa Over Breach, Bloomberg Business, (Aug. 18, 2015, 5:59 PM), http://www.bloomberg.com/news/articles/2015-08-18/target-says-it-has-reached-settlement-with-visa-over-data-breach (last updated Aug. 18, 2015, 5:59 PM).
60 Tina Orem, Target Suit Wins Class Action Status, Credit Union Times, (Sept. 15, 2015), http://www.cutimes.com/2015/09/15/target-suit-wins-class-action-status.
61 See Collier v. Steinhafel, No. 0:14-CV-00266, 2014 WL 321798 (D. Minn. Jan. 29, 2014).
62 *Id.*
63 See, *e.g.*, Protecting Personal Consumer Information from Cyber Attacks and Data Breaches: Hearing Before the S. Comm. On Commerce, Sci., & Transp., (Mar. 26, 2014), *available at* https://corporate.target.com/_media/TargetCorp/global/PDF/Target-SJC-032614.pdf (written testimony of John Mulligan, Executive V.P. and C.F.O., Target); see also Under Attack: Federal Security and the OPM Data Breach: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs, (June 25, 2015), *available at* https://www.opm.gov/news/testimony/114th-congress/under-attack-federal-cybersecurity-and-the-opm-data-breach.pdf (statement of Hon. Katherine Archuleta, Director, U.S. Office of Personal Management).
64 See Susan Taylor et al., Target's Decision to Remove CEO Rattles Investors, Reuters, (May 5, 2014, 5:32 PM), http://www.reuters.com/article/2014/05/05/us-target-ceo-idUSBREA440BD20140505.
65 Paul Ziobro & Joann S. Lublin, ISS's View on Target Directors Is a Signal on Cybersecurity, Wall St. J., http://www.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278 (last updated May 28, 2014, 6:28 PM).
66 Nelson & Tau, *supra* note 9.
67 Commissioner Luis A. Aguilar, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Cyber Risks and the Boardroom Conference, New York Stock Exchange (June 10, 2014), *available at* http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.
68 U.S. Dep't of Just., Cybersecurity Unit, http://www.justice.gov/criminal-ccips/cybersecurity-unit (last updated May 26, 2015).
69 Cybersecurity Unit, Best Practices for Victim Response and Reporting of Cyber Incidents, U.S. Dep't of Just. (April 2015), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.
70 U.S. Dep't of Just., Cybersecurity Unit, http://www.justice.gov/criminal-ccips/cybersecurity-unit (last updated May 26, 2015).
71 See Cybersecurity Unit, Best Practices, *supra* note 69 at 5; Fed. Bureau of Investigation, FBI – Computer Intrusions, https://www.fbi.gov/about-us/investigate/cyber/computer-intrusions.
72 U.S. Dep't of Homeland Sec., Combating Cyber Crime, http://www.dhs.gov/topic/combating-cyber-crime (last updated Sept. 23, 2015).
73 Noeleen Walder, Jonathan Stempel, & Joseph Ax, Hackers Stole Secrets For Up to $100 Million Insider-Trading Profit: U.S., Reuters, (Aug. 12, 2015, 5:02 AM),

http://www.reuters.com/article/2015/08/12/us-cybercybersecurity-hacking-stocks-arr-idUSKCN0QG1EY20150812.

74 Press Release, Fed. Bureau of Investigations , Major Computer Hacking Forum Dismantled, (July 15, 2015), https://www.fbi.gov/pittsburgh/press-releases/2015/major-computer-hacking-forum-dismantled.

75 *Id.*

76 Press Release, U.S. Dep't of Just., Manhattan U.S. Attorney and FBI Assistant Director-In-Charge Announce Charges In Connection with Blackshades Malicious Software That Enabled Users Around The World to Secretly And Remotely Control Victims' Computers (May 19, 2014), http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection.

77 Sarah N. Lynch, U.S. SEC on the Prowl for Cyber Security Cases—Official, Reuters, (Feb. 20, 2015, 4:07 PM), http://www.reuters.com/article/2015/02/20/sec-cyber-idUSL1N0VU2AV20150220 (quoting David Glockner).

78 *Id.*

79 CF Disclosure Guidance: Topic No. 2, Cybersecurity, Div. of Corp. Fin., U.S. Sec. & Exch. Comm'n (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

80 *Id.*

81 *Id.*

82 *Id.*

83 *Id.*

84 *Id.*

85 See Letter from Mary Jo White, Chair, Sec. & Exch. Comm'n, to Hon. John D. Rockefeller IV, Chairman, U.S. S. Comm. on Commerce, Sci., & Transp., (May 1, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=7b54b6d0-e9a1-44e9-8545-ea3f90a40edf (stating that "the staff issued comments addressing cybersecurity matters to approximately 50 public companies of varying size and in a wide variety of industries"); see, *e.g.*, Letter from Karl Hiller, Branch Manager, to Ira M. Birns, Exec. Vice President and Chief Fin. Officer, World Fuel Services Corp. (Mar. 20, 2015), *available at* http://www.sec.gov/Archives/edgar/data/789460/000000000015016935/filename1.pdf; Letter from Mara L. Ransom, Assistant Dir., to Jon Kessler, President and Chief Fin. Officer, HealthEquity, Inc. (May 1, 2014), *available at* http://www.sec.gov/Archives/edgar/data/1428336/000000000014022132/filename1.pdf;Letter from Linda Cvrkel, Branch Chief, to Joseph Ceryanec, Chief Fin. Officer, Meredith Corp. (Feb. 6, 2014), *available at* http://www.sec.gov/Archives/edgar/data/65011/000000000014006410/filename1.pdf.

86 See, *e.g.*, Cory Bennett, SEC Weighs Cybersecurity Disclosure Rules, The Hill, (Jan. 14, 2015, 6:00 AM), http://thehill.com/policy/cybersecurity/229431-sec-weighs-cybersecurity-disclosure-rules.

87 Division of Investment Management, U.S. Sec. & Exch. Comm'n, http://www.sec.gov/divisions/investment/investment_about.shtml (last updated Aug. 1, 2013).

88 Office of Compliance Inspections and Examinations, U.S. Sec. & Exch. Comm'n, http://www.sec.gov/ocie (last updated Sept. 22, 2015).

89 Div. of Inv. Mgmt., U.S. Sec. & Exch. Comm'n, IM Guidance Update, No. 2015-02 (April 2015), *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf.

90 *Id.*

91 *Id.*

92 Office of Compliance Inspections & Examinations, U.S. Sec. & Exch. Comm'n, OCIE Cybersecurity Initiative, National Exam Program Risk Alert, Vol. IV, Issue 2 (Apr. 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.
93 *Id.*
94 Office of Compliance Inspections & Examinations, U.S. Sec. & Exch. Comm'n, Cybersecurity Examination Sweep Summary, National Exam Program Risk Alert, Vol. IV, Issue 4 (Feb. 3, 2015), *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.
95 *Id.*
96 See Target Hackers Broke in Via HVAC Company, KrebsonSecurity, (Feb. 5, 2014), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
97 Cybersecurity Examination Sweep Summary, *supra* note 94.
98 *Id.*
99 Office of Compliance Inspections & Examinations, U.S. Sec. & Exch. Comm'n, OCIE's 2015 Cybersecurity Examination Initiative, National Exam Program Risk Alert, Vol. IV, Issue 8 (Sept. 15, 2015), *available at* http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.
100 *Id.*
101 17 C.F.R. § 248.30(a).
102 See, *e.g.*, Order Instituting Admin. and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Sec. Exch. Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order, In re Marc. A. Ellis, Sec. Exch. Act Release No. 64220, File No. 3-14328 (Apr. 7, 2011), *available at* http://www.sec.gov/litigation/admin/2011/34-64220.pdf; Letter of Acceptance, Waiver, and Consent, Dept. of Enforcement, Fin. Indus. Reg. Auth., No. 20080152998, In re D.A. Davidson & Co. (Apr. 9, 2010), *available at* http://www.securityprivacyandthelaw.com/uploads/file/4_9_2010%20FINRA%20Letter%20of%20Acceptance.pdf; Order Instituting Admin. and Cease-and-Desist Proceedings Pursuant to Sections 15(b) and 21c of the Sec. Exch. Act of 1934 and Sections 203(e) and 203(k) of the Inv. Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order as To LPL Financial Corp., In re LPL Financial Corp., Sec. Exch. Act Release No. 58515, File No. 3-13181 (Sept. 11, 2008), *available at* http://www.sec.gov/litigation/admin/2008/34-58515.pdf.
103 See Lynch, *supra* note 77.
104 Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach (Sept. 22, 2015), http://www.sec.gov/news/pressrelease/2015-202.html.
105 *Id.*
106 *Id.*
107 See Sec. & Exch. Comm'n Release No. 34-73639, File No. S7-01-13, RIN 3235-AL43 (Nov. 19, 2014), *available at* http://www.sec.gov/rules/final/2014/34-73639.pdf.
108 *Id*; see also 17 C.F.R. § 242 (2015).
109 Fin. Indus. Regulatory Auth., Report on Cybersecurity Practices (Feb. 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.
110 News Release, Fin. Indus. Regulatory Auth., FINRA Fines D.A. Davidson & Co. $375,000 for Failure to Protect Confidential Customer Information (Apr. 12, 2010), http://www.finra.org/newsroom/2010/finra-fines-da-davidson-co-375000-failure-protect-confidential-customer-information.

111 News Release, Fin. Indus. Regulatory Auth., Disciplinary and Other FINRA Actions, at 11 (July 2015), http://www.finra.org/sites/default/files/publication_file/July_2015_Disciplinary_Actions.pdf.
112 Emily Field, FCC Head Says Companies Must Be Cybersecurity Leaders, Law360, (Apr. 22, 2015, 6:19 PM), http://www.law360.com/articles/646465/fcc-head-says-companies-must-be-cybersecurity-leaders.
113 Sue Reisinger, FCC Fines AT&T $25M: Agency's Largest Cyber Enforcement, Corporate Counsel, (Apr. 14, 2015), http://www.corpcounsel.com/id=1202723349349/FCC-Fines-AT38T-3625M-Agencys-Largest-Cyber-Enforcement?slreturn=20150816162248.
114 *Id.* (quoting the FCC).
115 HIPAA Administrative Simplification Statute and Rules, U.S. Dep't of Health & Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html.
116 News Release, U.S. Dep't of Health & Human Services, Data Breach Results in $4.8 million HIPAA Settlements (May 7, 2014), http://www.hhs.gov/news/press/2014pres/05/20140507b.html.
117 Gigi Stevens, Cong. Research Serv., The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority 6 (Sept. 11, 2014), https://www.fas.org/sgp/crs/misc/R43723.pdf; see also *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime: Hearing Before the S. Comm. on the Judiciary*, (Feb. 4, 2014), (statement of Chairwoman Edith Ramirez), *available at* https://www.ftc.gov/system/files/documents/public_statements/oral-statement-federal-trade-commission-privacy-digital-age-preventing-data-breaches-combating/2014-02-04_judiciary_opening_statement_final.pdf.
118 *See* FTC v. Wyndham Worldwide Corp., No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015).
119 *Id.* at *7.
120 FED. TRADE COMM'N, FTC FACTS FOR BUSINESS: COMPLYING WITH THE FTC'S HEALTH BREACH NOTIFICATION RULE 1 (Apr. 2010), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus56-complying-ftcs-health-breach-notification-rule.pdf.
121 *Id.*
122 Matthew Goldstein, *State Attorneys General Press JPMorgan for More Details on Hacking*, N.Y. TIMES, (Jan. 14, 2015, 12:35 PM), http://dealbook.nytimes.com/2015/01/14/state-attorneys-general-press-jpmorgan-chase-for-more-details-on-hacking.
123 Cory Bennett, *State AGs Clash with Congress Over Data Breach Laws*, THE HILL, (July 7, 2015, 5:32 PM), http://thehill.com/policy/cybersecurity/247118-state-ags-warn-congress-against-preempting-data-breach-laws.
124 FIN. STABILITY OVERSIGHT COUNCIL, 2015 ANNUAL REPORT 102 (2015), *available at* http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf.
125 *Id.* at 3.
126 *Id.* at 9.
127 OFFICE OF THE COMPTROLLER OF THE CURRENCY, SEMIANNUAL RISK PERSPECTIVE FROM THE NATIONAL RISK COMMITTEE, (Spring 2015), *available at* http://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2015.pdf.
128 *Id.* at 10.
129 Sarah Dahlgren, Exec. Vice President, Fed. Reserve Bank of N.Y., Remarks at the OpRisk North America Annual Conference, New York City (Mar. 24, 2015), *available at* http://www.newyorkfed.org/newsevents/speeches/2015/dah150324.html.
130 McKendry & Macheel, *supra* note 12.

131 GAO-15-509, *supra* note 19, at 19-20
132 *Id.* at 20-21.
133 *Id.* app. 2, at 55-59.
134 12 C.F.R. Pt. 30, App. B (2014).
135 *Id.*
136 *Id.*
137 15 U.S.C. § 6801(b).
138 *See* Patco Const. Co. v. People's United Bank, 684 F.3d 197, 213 (1st Cir. 2012) (holding that bank's security procedures were not "commercially reasonable" based, in part, on the bank's failure to implement FFIEC guidance).
139 PONEMON INSTITUTE, *2015 Cost of Data Breach Study: Global Analysis,* IBM 1 (May 2015), http://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.pdf.
140 Commissioner Luis A. Aguilar, *supra* note 67.
141 LARRY CLINTON, NAT'L ASS'N OF CORP. DIRECTORS, *Cyber-Risk Oversight, Director's Handbook Series* 4 (2014), *available at* https://na.theiia.org/standards-guidance/Public%20Documents/NACD-Financial-Lines.pdf.
142 FED. FIN. INST. EXAMINATION COUNCIL, *FFIEC Cybersecurity Assessment Tool, Overview for Chief Executive Officers and Boards of Directors* (June 2015), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.
143 Fed. Fin. Insts. Examination Council, *supra* note 142, at 2.
144 PWC, *US Cybersecurity*, *supra* note 1, at 10.
145 Press Release, Office of the Press Sec'y, Fact Sheet: Administration Cybersecurity Efforts 2015 (July 9, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015.
146 Banks are positioned differently than most other companies because they have to defend against the threat on two fronts: (1) their own networks, and (2) fraudulent charges or transfers/withdrawals out of a customer's account when the *customer* has been the victim of a data breach elsewhere. Security measures that address the latter can impose additional burdens on customers, which raises other concerns, but it is fair to expect that they too will become more accustomed to—and more accepting of—some added inconvenience for the sake of enhanced security given the current climate.
147 GAO-15-509, *supra* note 19.
148 *Id.* at 24-25.
149 *Id.* at 45.
150 James O'Toole, *JPMorgan: 76 Million Customers Hacked,* CNN MONEY, (Oct. 3, 2014, 8:00 AM), http://money.cnn.com/2014/10/02/technology/security/jpmorgan-hack.
151 Emily Glazer, *J.P. Morgan CEO: Cybersecurity Spending to Double*, WALL ST. J., http://www.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976 (last updated Oct. 10, 2014, 5:57 PM).
152 GAO-15-509, *supra* note 19, at 1.
153 *See id.* at 13.
154 *Id.* at 27.
155 *Id.* at 28.
156 *Id.* at 29.
157 *Id.*
158 *Id.*
159 *Id.* at 33.

160 Cybersecurity Examination Sweep Summary, supra note 94, at 4.
161 GAO-15-509, *supra* note 19, at 34.
162 Testimony of Wm. Douglas Johnson, *supra* note 25.
163 GAO-15-509, *supra* note 19, at 34.
164 *Id.*
165 MANDIANT, A View From The Front Lines, supra note 18, at 1.
166 GAO-15-509, *supra* note 19, at 39.
167 *Id.*
168 *Id.*
169 VERIZON, *Data Breach Investigations Report*, *supra* note 17, at 10-11 (citing Risk Analytics data).
170 GAO-15-509, *supra* note 19, at 42.
171 *Treasury's Raskin Focusing on Improving Cyber Info-Sharing*, ABA BANKING JOURNAL, (July 14, 2015), http://bankingjournal.aba.com/2015/07/treasurys-raskin-focusing-on-improving-cyber-info-sharing (quoting Raskin).
172 GAO-15-509, *supra* note 19.
173 Exec. Order No. 13,691, 80 Fed. Reg. 9349 (Feb. 13, 2015).
174 Ellen Nakashima & Katie Zezima, *Obama to Propose Legislation to Protect Firms that Share Cyberthreat Data*, Wash. Post, (Jan. 12,2015), http://www.washingtonpost.com/politics/obama-proposes-legislation-to-protect-consumer-data-student-privacy/2015/01/12/539c4a06-9a8f-11e4-bcfb-059ec7a93ddc_story.html.
175 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong., 1st Session (2015); Protecting Cyber Networks Act, H.R. 1560, 114thCong. 1st Session (2015); National Cybersecurity Protection Advancement Act, H.R. 1730, 114th Cong., 1st Session (2015).
176 Fed. Fin. Inst. Examination Council, *supra* note 142, at 1.
177 *Id.* at 11.
178 *Id.* at 19-57.

Joseph Wayland

Executive Vice President and General Counsel
Chubb Limited / Chubb Group

Joseph Wayland is Executive Vice Preesident and General Counsel of Chubb Limited. He is responsible for the company's global legal affairs and serves as principal counsel to the CEO, senior management team and board of directors. Mr. Wayland also leads the legal organization that supports Chubb's business operations globally and is responsible for all legal functions, including corporate affairs and securities, litigation, compliance, and regulatory and government affairs. He also serves as secretary to the Chubb Limited Board of Directors.

Prior to ACE's acquisition of Chubb in January 2016, Mr. Wayland was the General Counsel of ACE Limited, a position he held since joining the company in 2013. He was appointed Executive Vice President, ACE Group, in March 2014.

Before joining ACE, Mr. Wayland was with Simpson Thacher & Bartlett, where he worked from 1988 and became a partner in 1994. From 2010 to 2012, he served in the United States Department of Justice, first as Deputy Assistant Attorney General responsible for litigation for the Antitrust Division, and was later appointed as the Acting Assistant Attorney General in charge of the division. Earlier in his career, Mr. Wayland served as a Captain in the United States Air Force.

Mr. Wayland holds a Juris Doctor degree from Columbia University Law School and a Bachelor of Arts degree from Washington University. He also holds a Master of Laws degree in International and Comparative Law from Georgetown University Law School. Mr. Wayland is a Fellow of the American College of Trial Lawyers.

Paul|Weiss

Elizabeth M. Sacksteder
Partner

Tel: 212-373-3505
Fax: 212-492-0505
esacksteder@paulweiss.com

New York
1285 Avenue of the Americas
New York, NY 10019-6064

Education
J.D., Yale Law School, 1988

A.B., Princeton University, 1980 summa cum laude, Phi Beta Kappa
Bar Admissions
New York

A partner in the Litigation Department, Elizabeth M. Sacksteder focuses her practice on complex litigation and regulatory matters.

Experience

Ms. Sacksteder is the former Deputy General Counsel and Global Head of Litigation and Regulatory Investigations at Citigroup Inc., where she managed a 250-person worldwide litigation and investigative team and advised Citigroup and its Board on every aspect of their litigation and regulatory exposures. During her tenure at Citigroup, Ms. Sacksteder supervised multibillion-dollar litigations and high-stakes regulatory and criminal investigations, many involving multiple jurisdictions. Prior to joining Citigroup, Ms. Sacksteder was the Deputy General Counsel and Director of Litigation at The Hartford Financial Services Group, Inc., where she was second in command in a 400-person Law Department. She was responsible for a 60-lawyer litigation group, all litigation and pre-litigation counseling involving the holding company and the group's property-casualty, life, and asset accumulation businesses, and supervision of the Reinsurance Law and Investment Law groups. Before joining The Hartford, Ms. Sacksteder was a litigation partner in private practice representing clients in financial services, telecommunications, manufacturing, entertainment, and other industries.

Ms. Sacksteder is a recipient of the Arthur Liman Public Interest Award from the Legal Action Center (2012) and the Human Relations Award from the New York Lawyers Division of the Anti-Defamation League (2013). Ms. Sacksteder serves as a Member of the Board of the Legal Action Center (2013 - present). She was the Coordinating Articles Editor of the Yale Law Journal.

Donald Hawthorne
Partner, Axinn, Veltrop & Harkrider LLP

Contact

TEL 212.261.5665
dhawthorne@axinn.com
New York

Don Hawthorne's practice focuses on litigation involving complex financial instruments, credit crisis litigation, antitrust litigation and counseling, and international disputes. He frequently represents insurers, hedge funds, and private equity firms, and represents both plaintiffs and defendants.

Don was previously with Debevoise & Plimpton. Prior to that, Don was Director of the e-Commerce Strategy Group at KPMG Consulting, Inc. From 1992 until 2000 Don was an associate and then Counsel with Paul, Weiss, Rifkind, Wharton & Garrison. Don has served as an Adjunct Associate Professor of Law at the Benjamin N. Cardozo School of Law, where for many years he taught courses on the regulation of electronic media covering legal issues concerning broadcast and cable media, the Internet and telephony. From 1991 until 1992 he was a law clerk to the Honorable H. Lee Sarokin of the District of New Jersey. And from 1986 until 1988 he was an associate with Booz, Allen & Hamilton in New York.

Professional Activities

- American Bar Association
- Association of the Bar of the City of New York

Edward Best joined Mayer Brown in 1986 and steadily built a successful capital markets and corporate law practice. Today, he is co-leader of the firm's Capital Markets and Financial Institutions groups and serves on Mayer Brown's Partnership Board. He is widely recognized as one of the nation's leading capital markets attorneys. Eddie's experience includes:

Capital Markets. Representing issuers and underwriters in connection with public and Rule 144A offerings of debt, equity, convertible and hybrid securities in the US and Europe; continuously offered debt and equity programs; liability management transactions, including equity and debt self-tenders, exchange offers, and consent solicitations; particular emphasis on offerings by financial institutions, including banks, insurance companies, brokers and specialty finance companies, and cross-border offerings.

Mergers and Acquisitions. Counseling buyers, sellers, and financial intermediaries in connection with public and private acquisitions, joint ventures, divestitures, mergers, tender offers, and proxy contests.

General Corporate Practice. Advising companies regarding Securities Act and Exchange Act compliance, NYSE and NASDAQ compliance, corporate governance, and Sarbanes-Oxley Act matters.

Chambers USA noted that "Edward Best's 'extremely quick mind' makes him a popular figure among lawyers and clients alike. 'He is never stumped by a question . . ..'" Eddie has been described as "Aptly named, as he's one of the best in town," and as "A 'stand-out debt and equity' lawyer." *Legal500* recommended Eddie in "Capital Markets - Debt Advice to Issuers" and "Capital Markets - High-Yield - Advice to Managers," noting that Eddie is "chief amongst [Mayer Brown's excellent partners]." Eddie is also listed in *Who's Who Legal, Best Lawyers in America* for Securities Law, the *Guide to the World's Leading Capital Market Lawyers*, *The International Who's Who of Capital Markets Lawyers* (2007), and the *International Who's Who of Business Lawyers* (2008). In addition, he has been named among the "Leading Lawyers" in Illinois in the categories of Corporate Finance Law, Mergers and Acquisitions Law, and Securities and Venture Finance Law.