Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 5 | Issue 1 Article 6

2010

Payments Data Security Breaches and Oil Spills: What Lessons Can Payments Security Learn From the Laws Governing Remediation of the Exxon Valdez, Deepwater Horizon, and Other Oil Spills

Sarah Jane Hughes

PAYMENTS DATA SECURITY BREACHES AND OIL SPILLS: WHAT LESSONS CAN PAYMENTS SECURITY LEARN FROM THE LAWS GOVERNING REMEDIATION OF THE EXXON VALDEZ, DEEPWATER HORIZON, AND OTHER OIL SPILLS?

Sarah Jane Hughes[*]

Legal regimes for remediating defects and certain accidents range from strict liability in tort to warranty enforcement litigation to international treaties and conventions with explicit, pre-ordained compensation limits and procedures. Although to date no over-arching legal regime has governed data security defects and breaches in the United States or elsewhere, data security breaches are as capable of inflicting externalities on counter-parties and consumers as the types of defects and accidents that are covered by such schemes.[1]

 Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law at the Maurer School of Law, Indiana University, Bloomington, Indiana. Professor Hughes would like to thank Professor Edward (Ted) Janger and Brooklyn Law School for the invitation to present this Article as part of the Data Security and Data Privacy in the Payment System Symposium, Dean Lauren Robel and the Maurer School for research support for it, and the other participants in this Symposium, the faculty of Brooklyn Law School, and the editors of the Brooklyn Journal of Corporate, Financial & Commercial Law for their helpful comments and camaraderie. I also thank Fred H. Cate, Distinguished Professor of Law and Director of the Center for Applied Cybersecurity Research, Indiana University, Roland L. Trope, and Stephen T. Middlebrook for conversations about aspects of this Article; Professor Edward Robertson of the Indiana University School of Informatics for assistance with the concept of how an analogy to a double-hulled vessel would work in the field of data security; and John P. Lowrey and Sean P. Giambattista, Maurer School of Law Classes of 2010 and 2011, respectively, for research assistance. Special thanks go to Professor Frank Pasquale, Lofton Professor of Law, Seton Hall Law School, for his helpful commentary on the Symposium draft of this Article. His references to earlier e-commerce scholarship, including articles such as Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law,* 41 GA. L. REV. 1 (2006), which drew upon more traditional environmental law analogies, enlivened discussion at the Symposium, and his historical perspective persuaded me to try to make the connection between the maritime-environmental law solutions and possible approaches to payments data security more clearly. Despite all of this talented help, all mistakes here are my own.

This Article is dedicated to dear friends, Inez Janger, who coincidentally is Ted Janger's mother, and the late Peter Ghee. Ms. Janger's experience and extraordinary common sense have helped steer a unique non-profit organization successfully through very stormy seas that have had nothing to do with data security or oil spills. Mr. Ghee's long career in the oil industry, shipping and maritime law and his acumen and foresight helped bring about the International Convention for the Prevention of Pollution from Ships, which is known as MARPOL 73/78 and my acquaintance with it, which I discuss in this Article.

Research for this Article ended on August 2, 2010, which was the 105th day after the explosion on the BP Deepwater Horizon drilling platform and subsequent oil spill into the Gulf of Mexico.

1. *See* Chris J. Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J.L. & TECH. 2, 29–34 (2009).

When I began thinking about a paper for this Symposium, I was struck by the similarities and differences between data security breaches and maritime accidents, at least in terms of their substantial consequential and incidental damages. In payments data security, these damages include card cancellation and replacement expenses, database clean-up expenses, counter-party and customer business relation expenses, reputational injuries (including loss of customers and market capitalization to business counter-parties), and the risk of identity theft, damage to credit ratings, lost credit opportunities, and emotional distress to card or account holders.[2] In the maritime and exploration industries, these damages include damage to the environment, shore and sea life, and livelihoods.[3]

In particular, I began wondering about whether pollution and sea-worthiness analogies might exist between famous payments data security breaches—that Professors Edward Janger, one of our hosts, and Paul Schwartz, a faculty alumnus of Brooklyn Law School, called "data spills"[4]—such as TJX,[5] Hannaford Brothers,[6] and Heartland Payments, Inc.,[7] and famous maritime accidents such as the Torrey Canyon wreck,[8] the Exxon Valdez grounding,[9] and the BP Deepwater Horizon explosion.[10] This line of inquiry also led me to the 1973 and 1978 international conventions that were drafted in response to Torrey Canyon,[11] and to ponder whether the

---

2. *See* United States v. Karro, 257 F.3d 112, 121 (2d Cir. 2001) (discussing the human cost of identity theft, including emotional costs).

3. *See* Joe Stephens, *The Valdez's Unheeded Lessons; BP was Part of Alaska Response, but Decades Later Same Problems Persist*, WASH. POST, July 14, 2010, at A1.

4. *See generally* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches,* 105 MICH. L. REV. 913 (2007).

5. *See, e.g.*, Press Release, Fed. Trade Comm'n, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data (Mar. 27, 2008), http://www.ftc.gov/opa/2008/03/data sec.shtm [hereinafter Settlement of Separate Actions].

6. *See In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108 (D. Me. 2009).

7. *See* Linda McGlasson, *Heartland, Visa Announce $60 Million Settlement Funds Would Reimburse Card Issuers for Breach-Related Losses*, BANKINFOSECURITY (Jan. 8, 2010), http://www.bankinfosecurity.com/articles.php?art_id=2054.

8. *See In re* Barracuda Tanker Corp., 281 F. Supp. 228 (S.D.N.Y. 1968). The Torrey Canyon, an oil tanker carrying more than 119,000 tons of oil from the Persian Gulf to Wales, was stranded on the rocks off the southwestern coast of England, causing the Torrey Canyon's oil tanks to rupture and discharge oil into the Atlantic, polluting both shorelines of the English Channel. *See id.* at 229. The British Royal Air Force eventually bombed the Torrey Canyon, destroying the ship and leading to a total loss of its cargo. *Id.*

9. *See* Exxon Shipping Co. v. Baker, 128 S. Ct. 2605 (2008). The Exxon Valdez, a "supertanker" carrying 53 million gallons of oil from Alaska to the lower 48 states, "grounded on Bligh Reef off the Alaskan coast," causing the discharge of millions of gallons of crude oil into Prince William Sound after the ship's hull fractured. *Id.* at 2611–13.

10. *See* Campbell Robertson, *11 Remain Missing After Oil Rig Explodes Off Louisiana; 17 are Hurt*, N.Y. TIMES, Apr. 22, 2010, at A13.

11. *See Background on Pollution Prevention and MARPOL 73/78*, INTERNATIONAL MARITIME ORGANIZATION, http://www.imo.org/OurWork/Environment/PollutionPrevention/

core teachings of those conventions might help frame approaches for data security breach prevention, clean-up, and liability.

Just as Professor Juliet M. Moringiello's Article for this Symposium harks back to property law and common law warranties to suggest an approach for more contemporary payments data security breaches,[12] I recognize that data spills are newer phenomena than maritime accidents and oil spills. Thus, in searching for approaches to these problems, I, too, looked backwards—but to different sources of law. However, like accidents involving discharges of oil and other pollutants at sea, such as Exxon Valdez, and incidents involving problems with oil and gas exploration, such as Deepwater Horizon, data security breach remediation may require the development of laws, treaties, and conventions to govern these types of accidents.

Of course, at the March 19, 2010 Symposium at Brooklyn Law School, we had no idea that only a month later one of the most devastating oil spills in U.S. history would occur. The events surrounding the April 20, 2010 explosion on the BP Deepwater Horizon oil drilling platform in the Gulf of Mexico will be featured prominently in our discussions of energy policy, environmental policy, and general disaster management for decades,[13] just as the data security breaches at TJX, RBS WorldPay, and Heartland will in future discussions of data security policy.

The WellPoint data breach—disclosed in June, 2010[14]—and Hannaford highlight additional concerns with payments data risk management and data governance that had not been the focus of the Symposium draft of this Article. These concerns include a lack of coordinated rapid-fire response capacities and delays in sharing information about breaches with affected constituencies—including merchant banks and customers—that need it most.[15] Similarly, Deepwater Horizon confirmed that we still lacked sufficient rapid-fire disaster relief capability for natural disasters than was evident following Hurricane Katrina or Exxon Valdez.[16] In both data and natural disasters, we depend on private risk determinations pre- and post-accidents and largely private efforts to manage critical pieces of the recovery processes. The incentives of the companies that bear the largest

---

OilPollution/Pages/Background.aspx (last visited Dec. 27, 2010); *see also* International Convention for the Prevention of Pollution from Ships, 1973, *concluded* Nov. 2, 1973, 1340 U.N.T.S 184, 12 I.L.M. 1319, 1340, as modified by Protocol of 1978 Relating to the International Convention for the Prevention of Pollution from Ships, 1973, *concluded* Feb. 17, 1978, 1340 U.N.T.S 61, 17 I.L.M. 146 [hereinafter MARPOL 73/78].

12. Juliet Moringiello, *Warranting Data Security*, 5 BROOKLYN J. CORP. FIN. & COMM. L. 63 (2010).

13. *See* Stephens, *supra* note 3.

14. *See* Steve Ragan, *WellPoint: Data Breach Caused by Attorneys and Faulty Security Update*, TECH. HERALD (June 29, 2010, 6:11 PM), http://www.thetechherald.com/article.php/201026/5807/WellPoint-Data-breach-caused-by-attorneys-and-faulty-security-update.

15. *Id.*

16. *See* Stephens, *supra* note 3.

responsibility for oil spills are similar to the incentives of private payments systems and users that report payments data security breaches to authorities, and their nearly exclusive role in remedying the damages to others affected by payments data breaches.[17] Thus, we are all hostages in a sense to private decision-making in the prevention and remediation of certain events and to the rigorous cost-cutting that has typified business practice in the United States.[18] In addition, pending criminal investigations (or even the prospect of them) generally delay access to critical information about culpability. It often is some time before we can know the full details about accidents—whether oil spills or shipping mishaps, or data security breaches—and these delays themselves may slow the process of crafting appropriate protections and remediation schemes for the specific incidents and applying the lessons learned from each going forward.

The totality of ship and drilling accidents—of which, federal records suggest, a "handful" occurred in the Gulf of Mexico annually from 1964 to 2009,[19]—also sent me thinking beyond the negligent or criminal data security breach events that occupied most of my thinking prior to the Symposium. Broader transnational crimes, national security threats, and disaster management concerns present themselves in the payments data arena almost as starkly as in the maritime and environmental accidents arena.[20]

Much has been written about payments data security breaches and the damages they can impose on consumers who are victims.[21] Perhaps just as much has been written about various state laws and federal proposals that require providers to notify consumers when their personally identifiable information has been lost.[22] The quality of these articles leaves me free to

---

17. *See* Schwartz & Janger, *supra* note 4, at 919.

18. *See* Stephens, *supra* note 3; *see also* Hoofnagle, *supra* note 1, at 33.

19. Steven Mufson, *Since '64, A Steady Stream of Oil Spills Has Tainted Gulf*, WASH. POST, July 24, 2010, at A1.

20. In the days following the 9/11 World Trade Center attacks, the Federal Reserve System put hundreds of millions of dollars of liquidity into the U.S. banking system in order to keep the economy running. James J. McAndrews & Simon M. Potter, *Liquidity Effects of the Events of September 11, 2001*, FED. RESERVE BANK OF N.Y. ECON. POL'Y REV., Nov. 2002, at 59, *available at* http://www.newyorkfed.org/research/epr/02v08n2/0211mcan.pdf. The Federal Reserve lent billions of dollars through the discount window, more than 200 times the daily average amount of lending in the prior month, and temporarily waived daylight overdraft fees and overnight overdraft penalties. *Id.* at 69–70.

21. *E.g.*, J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 121–23 (2008); Chris J. Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J.L. & TECH. 97, 98 (2007); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003); Schwartz & Janger, *supra* note 4.

22. *See, e.g.*, Janine S. Hiller, David L. Baumer & Wade M. Chumney, *Due Diligence on the Run: Business Lessons Derived from FTC Actions to Enforce Core Security Principles*, 45 IDAHO L. REV. 283, 285–88, 305–08 (2009) (discussing international, federal, and state laws regarding hacking and privacy, and the application of legal principles to enhance consumer privacy); Bruce A. Colbath, *Customer Privacy & Data Security: The Importance of Guarding Your Hen-House*,

pursue other issues here; which, of course, does not suggest that I could handle them as well as their authors did.

But relatively less has been written about the "direct and indirect" damages and "opportunity costs" that payments systems participants suffer because of data spills.[23] These businesses normally are not the targets or entry points of data security breaches, but rather sustain forms of collateral "pollution" from those data security "spills"[24] much like maritime accidents pollute physical and environmental assets. These payment systems participants include entities upstream from a data security breach, as well as others on its periphery.[25] To complicate recovery of collateral costs borne in these cases, contractual disclaimers for third-party losses dominate in the major agreements governing the operation of the credit card systems.[26] They are less common in wire transfer bank-customer agreements because the Uniform Commercial Code (UCC)'s Article 4A regime requires an explicit agreement to pay consequential damages and also limits—to the extent allowed by Section 4A-305—the opportunity to vary the liability of the receiving bank by agreement.[27]

Data security in payments takes on a new urgency in light of reports about recent mass-scale hackings—including the hacking into Google Gmail accounts by the People's Republic of China[28]—reports that individuals based in China are hacking into commercial databases,[29] and reports about the increasing scope of criminal hacking episodes.[30] The

---

60 CONSUMER FIN. L. Q. REP. 603, 607 (2006) (discussing state statutes enacted in the wake of the Choicepoint data breach).

23. For an example of specific research addressing these issues, see PONEMON INSTITUTE, 2008 ANNUAL STUDY: COST OF A DATA BREACH (2009), *available at* http://www.encryptionreports.com/download/Ponemon_COB_2008_US_090201.pdf.

24. *See id.*

25. *See id.*

26. *See* VISA, RULES FOR VISA MERCHANTS: CARD ACCEPTANCE AND CHARGEBACK MANAGEMENT GUIDELINES 60 (2007), *available at* http://www.emscard.com/uploads/Documents/rules_for_visa_merchants.pdf.

27. U.C.C. § 4A-305 (2001). Of course, UCC Article 4A also sets forth a series of rules that are designed to allow the receiving bank to identify erroneous payment orders by reliance on specific arrangements in the security procedure agreed to by the sender and its receiving bank. *E.g.*, *id.* § 4A-205 (2001). The sender also has a duty to discover and report errors in orders accepted by the receiving bank. *Id.* § 4A-205(b). In addition, in connection with a claim for liability for late or improper execution or failure to execute payment orders, § 4A-305(a) of the U.C.C. limits damages to those payable under subsections (a) and (b). Other damages, including consequential damages, are recoverable to the extent provided in an express written agreement of the receiving bank. *Id.* § 4A-305(c)–(d).

28. *See, e.g.*, *A New Approach to China*, THE OFFICIAL GOOGLE BLOG (Jan. 12, 2010, 3:00 PM), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

29. Mike Harvey, *China Raid on Google 'Also Hit Global Industrial Targets'; Hackers Installed 'Back Door' to Gain Control of Computers*, TIMES (UK), Jan. 16, 2010, at 15.

30. *Id.* In contrast, the combined number of data security breaches reported by government and military agencies in the United States fell in 2009 compared with 2008, but the number of records affected was larger. Hilton Collins, *Many More Government Records Compromised in 2009 than Year Ago, Report Claims,* GOV'T TECH. (Dec. 2, 2009),

cross-border aspects of such breaches add to this urgency,[31] particularly because they make business-to-business (B2B) and business-to-consumer (B2C) compensation more complicated.[32] Additional concerns emerge from the prospect of strategic hacking incidents, including the lack of apparent well-coordinated disaster response and management capacity, and the continued reliance on private actors to prevent, report, and respond to data security breaches.[33]

We also must confront the fact that many cyber-breaches are never publicized to persons whose information may have spilled or to law enforcement.[34] In some cases, even incidents that are publicized in news media may not be revealed with particularity to customers. For example, following Heartland, my family received new credit cards in the mail with new account numbers and no explanation whatsoever from the card issuers of why they suddenly were replacing cards that had not expired. In early 2010, I received a new set of American Express cards bearing the same expiration date also with no explanation; concerned, I called the company and learned that the replacements were part of its private remediation of a former employee's theft of hard drives containing many thousands of cardholders' personal information that had been detected nine months prior. Apparently to reassure me, the company's representative told me that the perpetrator was now cooperating with the recovery efforts and that my account data had only recently been identified as having been affected by the theft.

---

http://www.govtech.com/gt/articles/734214 (discussing a report by the Identity Theft Resource Center that the number of breaches reported up to December 2009 was 82 compared with 110 for all of 2008 but that the number of records affected soared from less than three million to more than 79 million). The report apparently called for greater vigilance in securing data, including "when it's mobile." *Id.* The article also cited 461 separate data breaches in "all sectors" affecting 222 million records, as opposed to a total of 656 breaches in 2008 that affected "more than 35 million compromised records." *Id.*

31. William Resnik et al., *Wave of Online Banking Fraud Targeting Businesses,* K&L GATES NEWSSTAND (Feb. 15, 2010), http://www.klgates.com/newsstand/detail.aspx?publication=6209 (explaining the growing theft and misuse of user names and passwords to online banking accounts and use of fraudulent wire transfers and automated clearing house (ACH) transfers to foreign countries).

32. *See id.* The terms "B2B" and "B2C" refer, respectively, to business-to-business and business-to-consumer transactions in e-commerce and e-payments. *See, e.g.*, Jane K. Winn, *Consumers and Standard Setting in Electronic Payments Regulation,* 5 ELEC. BANKING L. & COM. REP. 11, 15 (2002)*;* Robert Kossick, *The Internet in Latin America: New Opportunities, Developments, & Challenges,* 16 AM. U. INT'L L. REV. 1309, 1310 (2001).

33. *See* Ellen Nakashima, *War Game Reveals U.S. Lacks Cyber-Crisis Skills; Staged Emergency Displays Need for Strategy, Organizers Say*, WASH. POST, Feb. 17, 2010, at A3 (covering the February 2010 "Cyber Shock Wave" simulation conducted in Washington, D.C.).

34. *See* Diane Bartz & Jim Finkle, *Cyber Breaches Are a Closely Kept Secret,* REUTERS, Nov. 24, 2009, *available at* http://www.reuters.com/article/idUSTRE5AN4YH20091124 (detailing the reluctance of companies that are victims of breaches to disclose them because of fear of reputational damage, loss of customers, injury to profits, and criminal attention shifting to smaller and medium-sized firms whose data is less well protected).

Finally, in a reminder that seemingly ordinary burglaries may cause massive expenses and potential liability, on March 1, 2010, a report emerged about an October 2, 2009 burglary of fifty-seven hard drives from a closet at a BlueCross BlueShield of Tennessee training facility.[35] These hard drives apparently contained unencrypted data from more than one million customer support calls and 300,000 "screen shots" of computer monitors made contemporaneously with the support calls; most of the calls and many screen shots revealed sensitive personal information that is used in identity theft, according to the report.[36]

The Ponemon Institute's annual report on data breach costs suggests that the overwhelming percentage of breaches is attributable to negligence by insiders.[37] Negligence in the handling of sensitive personal information in transmission or storage is not dissimilar from the captain's absence from the bridge as the Exxon Valdez approached the reefs in Prince William Sound, Alaska with an inebriated harbor pilot at the controls,[38] or the series of "risk-based decisions" that BP apparently made in the management of the drilling process at the Deepwater Horizon facility and for which government investigators tentatively concluded that the operators chose the "least expensive option even though it potentially elevated the risk."[39] So, in the prevention of oil spills, one commentator observed the lessons we ought to have learned from the grounding of the Exxon Valdez went "unheeded" too long.[40] The same may be said of data spills because of the slow pace of U.S. card security to adopt Europay, MasterCard, and Visa (EVM) security, and this may involve risk assessments that opt for less expensive technologies over those that offer greater security for data.[41]

---

35. Robert McMillan, *Data Theft Creates Notification Nightmare for BlueCross,* PCWORLD (Mar. 1, 2010, 5:30 PM), http://www.pcworld.com/businesscenter/article/190461/data_theft_creates_notification_nightmare_for_bluecross.html [hereinafter McMillan, *Data Theft*].

36. *Id.* (detailing more than five months of work including notification of more than 300,000 customers so far and expenses of more than $7 million).

37. PONEMON INSTITUTE, *supra* note 23, at 7.

38. *See* Stephens, *supra* note 3. For more detailed information about the Exxon Valdez grounding, oil spill, and its causes, see ALASKA OIL SPILL COMMISSION, SPILL: THE WRECK OF THE EXXON VALDEZ, IMPLICATIONS FOR SAFE TRANSPORT OF OIL (1990), *available at* https://www.washingtonpost.com/wp-srv/special/oil-spill/docs/alaska-commission-report.pdf.

39. Joel Achenbach & David Hilzenrath, *From Series of Missteps to Calamity in the Gulf; Investigators Believe that BP Cut Corners*, WASH. POST, July 25, 2010, at A1.

40. Stephens, *supra* note 3 (reporting on BP predecessor British Petroleum's "central role" in the Exxon Valdez incident and pointing a finger at cost-cutting to maximize profits and regulators "too close to the oil industry" that "approved woefully inadequate accident response and cleanup plans"). Stephens also described comments made by the Chairman of the former Alaska Oil Spill Commission, Walt Parker, including "'[i]t's almost as though we had never written the report [on the Exxon Valdez].'" *Id.*

41. Kate Fitzgerald, *Fraud Could Come from North After Canada Phases in EMV,* AM. BANKER, July 14, 2010, at 6 (citing a prediction by Christopher Justice, the president for North America of the French payment terminal maker Ingenico S.A., that "'fraudsters specializing in magnetic stripes will begin to focus more heavily on the U.S. as Canada moves away from mag-

This Article suggests sources of law for an institutional framework that would create stronger incentives for the prevention of payments data breaches and for their prompt remediation, including a requirement for compulsory notice to a central agency regardless of the number of individuals or records involved. It does not advocate compulsory notice to consumers whose rights may be affected by a cyber-security breach, and instead recommends that the central agency—whether domestic or international—decide whether notifying consumers whose accounts might be affected is warranted. The Article also considers whether our current means of redressing losses through payments system rules and litigation is preferable to possible federal schemes like the oil liability provisions of the Clean Water Act,[42] and the liability provisions of the Oil Pollution Act (OPA) of 1990.[43] The former established strict liability civil penalties and significantly higher civil penalties for cases involving gross negligence.[44] The latter establishes a liability framework that increases incentives for prevention by limiting damages to removal costs and maximum damages unless the oil spill incident was caused by the gross negligence or willful misconduct of the responsible party or the failure or refusal of the responsible party or its counter-parties to report the incident.[45] If the liability limits are too low, the tendency will be either to devote too few resources to prevention, or to fail to report or underreport the severity of the spill, as may have happened in Deepwater Horizon.[46] Incomplete or delayed notice requirements in the data spills hinder remediation and may contribute to broader complications, including threats to larger payments systems and critical infrastructure. Reporting delays or incomplete reporting would particularly complicate the remediation of malicious attacks or strategic behavior designed to cripple part or all of the domestic payments systems.

Part I of this Article briefly describes what government agencies, think tanks, and the media have reported about recent high-profile data spills affecting payments systems, and particularly the prospects of large-scale criminal and even strategic cyber-security threats.[47] Part II describes the

---

stripe'" and also that converting "back-office and software . . . to switch from mag-stripe card would cost billions" as an explanation of the slower pace of EMV adoption here).

42. Federal Water Pollution Control Act (Clean Water Act), 33 U.S.C. §§ 1251–1321 (2006).

43. Oil Pollution Act of 1990, 33 U.S.C. §§ 2702, 2704 (2006).

44. *Compare* 33 U.S.C. § 1321(7)(A) (strict liability civil penalty), *with* 33 U.S.C. § 1321 (7)(D) (significantly higher civil penalty for cases involving gross negligence). However, neither penalty was sufficiently large to deter the cost-cutting and low-balled risk assessments that allegedly led to the Deepwater Horizon explosion.

45. *Compare* 33 U.S.C. § 2704(a)(3) (maximum liability and removal costs for offshore facilities is "the total of all removal costs plus $75,000,000"), *with* 33 U.S.C. § 2704(c)(1)–(2) (the prior limit is inapplicable if the incident is proximately caused by gross negligence or willful misconduct, or involves a violation of a federal safety, construction, or operating regulation, or if the responsible party does not report the incident).

46. *See* Mufson, *supra* note 19.

47. *See* Nakashima, *supra* note 33.

origins of the International Convention for the Prevention of Pollution from Ships 1973, as modified by the Protocol of 1978 relating thereto, collectively known as MARPOL 73/78,[48] in major pollution events associated with maritime accidents and particularly the Convention's requirements for the prevention of pollution. It also describes the federal Clean Water Act, which prescribes rules for spills from pipelines as well as oil wells,[49] and the OPA, which prescribes special rules for off-shore facilities and deepwater ports spill liability.[50] Part III compares the requirements and remedies that MARPOL and the OPA offer with those available for the prevention of data security breaches. Part IV evaluates recently passed and introduced bills focused on data security breaches and cyber-security problems generally. It also briefly discusses recent state legislation relating to data security breaches. Part V asks whether "safe harbor" provisions in legislation might result in reduced prevention and less effective care to recover from data spills rather than more. Part VI sets forth conclusions.

I. PAYMENTS DATA SECURITY BREACHES/DATA SPILLS

Like maritime or oil exploration accidents discharging oil or other pollutants, data security breaches come in many sizes.[51] However, unlike the provisions of the OPA that specifically allow removal costs incurred in connection with oil spills into the navigable waters, adjoining waters, or the exclusive economic zone of the United States,[52] there is no comparable federal liability scheme for data spills. Accordingly, prevention plans and remediation efforts have largely been left to private actors in the data spill arena.[53] For example, the federal "Safeguards Rule" implementing Section 501 of the Gramm-Leach-Bliley Act (GLBA) Privacy provisions,[54] and the Disposal and Red Flags Rules implementing the Fair and Accurate Credit Transactions Act of 2003 (FACTA)[55] that apply to providers of consumer financial products and services, reflect legislative and regulatory preferences for self-assessments of risks and for implementation by private

48. MARPOL 73/78, *supra* note 11.

49. 33 U.S.C. § 1321.

50. 33 U.S.C. §§ 2701–2762 (2006).

51. Mark Jewell, *TJX Breach Could Top 94 Million Accounts*, MSNBC.COM, Oct. 24, 2007, http://www.msnbc.msn.com/id/21454847.

52. 33 U.S.C. § 2702(a)–(b)(1).

53. *See, e.g.*, Standards for Safeguarding Customer Information, 67 Fed. Reg. 36,484, 36,484 (May 23, 2002) (to be codified at 16 C.F.R. § 314).

54. *See* Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2010). § 501 privacy provisions that are the underlying authority for the Safeguards Rule are codified at 15 U.S.C. §§ 6801–6809 (2006).

55. Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft, 16 C.F.R. § 681.2 (2006); Disposal of Consumer Report Information and Records, 16 C.F.R. § 682 (2006). *See also* Fair and Accurate Credit Transactions Act (FACTA) of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended at 15 U.S.C. § 1681).

actors of policies and procedures that match these self-assessments.[56] State laws also leave to private actors the ability to own or license personal information about their customers, and implement and maintain "reasonable security procedures and practices," but require these procedures and practices to be "appropriate to the nature of the information" to protect it from "access, destruction, use, modification, or disclosure."[57] Thus, incentives exist for low-balling risk in order to reduce the costs associated with prevention of data security breaches, just as it appears that low-balled or ignored risks contributed to the well explosion and subsequent inability to control the oil spill from the Deepwater Horizon well.[58]

The next portion of this Article examines recent data spills and their remediation costs. These examples reflect different types of spills—some negligent and some presumptively criminal or malicious—and their effects in terms of unauthorized access to account information or loss of funds by some affected parties.

A. RECENT SPILLS INVOLVING PAYMENTS DATA

Four recent examples suggest that substantial damages may result from payments data breaches. These examples represent different problems that payments systems participants have with data security, including B2B liability and B2C liability, as well as qualifications to participate in payment systems.

1. WellPoint

WellPoint, Inc. (WellPoint) is the nation's largest health insurer with a customer base of more than 30 million.[59] It apparently experienced a data breach in October 2009, as the result of a failed security update.[60] WellPoint reports that the breach "could have exposed personal information," including medical history and payment information, "belonging to 470,000 customers."[61] WellPoint did not learn about the breach until it received a subpoena the following March.[62] The company attributed some unauthorized access to manipulation by attorneys representing an applicant

56. *See, e.g.*, Standards for Safeguarding Customer Information, 67 Fed. Reg. at 36,484 (final rule requires financial institutions to develop written information security programs appropriate to the size and complexity of their operation, the nature and scope of activities in which they engage, and the sensitivity of the customer information they obtain, and also that "certain basis elements" be included to "ensure that it addresses the relevant aspects of the financial institution's operations and that it keeps pace with developments that may have a material impact on its safeguards").

57. *E.g.*, CAL. CIV. CODE § 1798.81.5(b) (Deering 2009).

58. Achenbach & Hilzenrath, *supra* note 39.

59. *See* Ragan, *supra* note 14.

60. *Id.*

61. *Id.*

62. *Id.*

for insurance.[63] It had notified 470,000 customers—including 230,000 in California alone—by June 29, 2010, and had undertaken other remediation measures. WellPoint continued to access its options for the recovery of its expenses and data as it remains unclear precisely who or how many unauthorized persons gained access to the records.[64]

2. Royal Bank of Scotland

Data spills affecting the Royal Bank of Scotland (RBS) are a reminder that not all payments data spills target U.S. providers or consumers in the U.S. RBS has had more than one payments data security breach. In 2008, the company—along with American Express and UK-based NatWest Bank—lost data contained on a server that was sold on eBay for the equivalent of $64; the server apparently contained unencrypted back-up data "includ[ing] names, addresses, bank account numbers, telephone numbers and customer signatures."[65]

On November 8, 2008, RBS WorldPay experienced widespread fraud as a result of another data breach.[66] The data breach had occurred earlier when unauthorized individuals accessed the information.[67] This time, RBS lost $9 million when thieves used ATMs in forty-nine cities around the world to gain the cash after penetrating RBS WorldPay servers.[68] After stealing encrypted data from payroll cards and the associated PINs, some members of the group also allegedly accessed the RBS WorldPay network and raised the applicable limits on the cards as well as limits on what could be withdrawn at ATMs with the cards.[69] Following that breach, Visa stripped RBS of its status as a validated service provider, but by May 22, 2009, it had restored RBS' status as a Payment Card Industry Data Security Standard (PCI DSS) validated service provider.[70]

3. Helsinki, Finland Merchant

A second case concerning a non-U.S. owner of data involved a Helsinki, Finland merchant who reported that data from more than 100,000 payment cards had been stolen from the merchant's server; of these, 40,000

---

63. *Id.*

64. *Id.*

65. Tom Espiner, *Amex, Royal Bank of Scotland, NatWest Customer Details Sold on eBay,* CNET NEWS (Aug. 26, 2008, 10:57 AM), http://news.cnet.com/8301-1009_3-10026032-83.html.

66. Robert Lemos, *Data-Breach Lawsuit Follows $9 Million Heist,* SECURITYFOCUS (Feb. 6, 2009), http://www.securityfocus.com/brief/903.

67. *Id.*

68. *Id.*

69. *RBS WorldPay Indictment Outlines Sophisticated Hacker Coordination*, DIGITAL TRANSACTIONS (Nov. 11, 2009), http://www.digitaltransactions.net/index.php/news/story/2371.

70. Warwick Ashford, *RBS WorldPay Regains Security Approval After Data Breach*, COMPUTERWEEKLY (May 22, 2009, 9:25 AM), http://www.computerweekly.com/Articles/2009/05/22/236142/RBS-WorldPay-regains-security-approval-after-data-breach.htm.

were active cards.[71] The Helsinki Criminal Police's Information Technology Crimes Unit reported that: (a) the attacks on the merchant's servers were traced to internet protocol addresses in Romania and the United States although they were uncertain that the attacks originated in either country; (b) the data breach occurred in mid-January, but involved payment cards from 2005 to January 2010—as many as three-fifths of which may have expired; (c) a routine computer security check uncovered the breach; and (d) the merchant has removed the vulnerable system from use and has replaced it with the newer-age, less vulnerable EMV system.[72] The merchant had decided to notify only those domestic and foreign cardholders whose cards have been fraudulently used.[73] Finland's largest credit card services company, Luottokunta, noted that because Finnish merchants use the PCI DSS, advanced monitoring, and card shutdown systems, the level of payment card abuses was "half" the rate experienced in other countries.[74]

4. P2P File Sharing (Unnamed Victims or Potential Victims).

A fourth type of data spill apparently involves person-to-person (P2P) file sharing at almost 100 organizations, as reported by the Federal Trade Commission (FTC) in February 2010. The details about these data spills are vague, but the FTC's press release makes it clear that file sharing software enabled the transmission of personally identifiable and account information otherwise available on the computer on which the file-sharing programs were run.[75]

B. WHAT DO PAYMENTS DATA SPILLS COST?

As the above data security breaches suggest, reported costs for data security breaches have risen over the past few years. For example, the *2008 Annual Study: Cost of a Data Breach*, issued in February 2009, reported that "total annual costs" incurred in seventeen different industries rose to "$202 per record compromised [in 2008], an increase of 2.5 percent since 2007 ($197 per record) and 11 percent [since] 2006 ($182 per record)."[76] The same study reported that the largest cost increase involved "abnormal

71. Marcus Hoy, *Data Security: Payment Card Data Theft from Merchant is Finland's Largest Card Breach, Police Say*, 94 BNA BANKING REP. 443 (2010).

72. *Id.* An EMV system is a specialty security platform that Europay, MasterCard, and VISA use outside the United States; it features chip-and-PIN technology. *See* CARDLOGIX, SMART CARD & SECURITY BASICS 7 (2009), *available at* http://www.smartcardbasics.com/pdf/7100030_BKL_Smart-Card-&-Security-Basics.

73. Hoy, *supra* note 71.

74. *Id.*

75. Press Release, Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), http://www.ftc.gov/opa/2010/02/p2palert.shtm.

76. PONEMON INSTITUTE, *supra* note 23, at 4.

churn," which indicates customer turnover.[77] The report also noted that healthcare and financial services companies that experienced data breaches had the highest churn (customer defections) factors of 6.5 and 5.5 percent, respectively, which the report attributed to both the sensitivity of the data collected and customer expectations that information will be protected.[78]

Other factors in the overall costs of data spills identified in the Ponemon Institute report include "outlays for detection, escalation, notification, and after the fact (ex-post) response."[79] Companies that experience data security breaches—like those that experience oil spills—also suffer declines in their market capitalizations that can be significant.[80] Evidence suggests that payments-related data spills cost an average of more than $6.6 million.[81] TJX reported losses of more than $1 billion in connection with its 2006 breach,[82] and direct remediation expenses of $256 million.[83]And, in addition, companies that suffer payments data spills often experience significant declines in their capitalization in the period following report of the breach.[84]

These significant declines in capitalization appear to be in addition to the direct remediation costs reported above and costs associated with enforcement actions and instituting and maintaining compliance plans. FTC

---

77. *Id.*

78. *Id.*

79. *Id.* at 3.

80. *See, e.g.*, Jim Puzzanghera & Ronald D. White, *BP Courts Mideast Investors; Increased Stakes from the Region Could Hurt Its Image Further and Trigger U.S. Reviews*, L.A. TIMES, July 8, 2010, at A1 ("Solvency has been a concern as BP's stock value has plummeted as much as 55% since oil started spewing from the Gulf of Mexico well in April.").

Heartland Payments Systems, Inc. fared worse than TJX did in terms of market capitalization gyrations after their data security incidents. *Compare* Jaikumar Vijayan, *One Year Later: Five Takeaways from the TJX Breach,* COMPUTERWORLD (Jan. 17, 2008, 12:00PM), http://www.computerworld.com/s/article/9057758/One_year_later_Five_takeaways_from_the_TJX_breach ("Despite being the biggest, costliest and perhaps most written-about breach ever, customer and investor confidence in TJX has remained largely unshaken. TJX's stock was worth about $30 per share when the breach was disclosed, and its closing price today was just over $29."), *with* Todd Wallack, *Data Breach Ensnares Many in Mass.; Credit and Debit Card Numbers Compromised,* BOS. GLOBE, May 13, 2009, at B1 ("Heartland shares dropped sharply after the company disclosed the breach Jan. 20. The company's stock, which peaked at more than $18 per share in early January, fell rapidly in the days after the disclosure, going as low as $4 in March. It closed yesterday at $9.04."). When seeing such a disparity one is tempted to ask, is this disparity in investor reaction a measure of the likely differences between retailers that have goods to sell to consumers and data processors that exist in a different, highly competitive market but whose direct counter-parties are better able to move to another processor? Concerns over the effects on local economies of the Deepwater Horizon spill have caused worries for banks. *See* Rachel Witkowski, *Equity Flows Out of Fla. As Oil Seeps in*, AM. BANKER, July 15, 2010, at 1.

81. PONEMON INSTITUTE, *supra* note 23, at 4. Data breaches such as the BlueCross BlueShield of Tennessee breach are considered "more complex than a typical data breach," and are likely to cost more than the average amount. *See* McMillan, *Data Theft*, *supra* note 35.

82. Jeff Kress, *Is Your Information Safe?*, CA MAGAZINE, Aug. 1, 2008, at 44.

83. Ross Kerber, *Cost of Data Breach at TJX Soars to $256m—Suits, Computer Fix Add to Expenses*, BOS. GLOBE, Aug. 15, 2007, at A1.

84. PONEMON INSTITUTE, *supra* note 23, at 4.

enforcement actions involving violations of its financial privacy and safeguards rules, or pursuant to its unfair or deceptive practices authority, have required—in various combinations—civil penalties, consumer redress payments, implementation of comprehensive data security programs, and implementation of independent audits of compliance.[85] For example, ChoicePoint, Inc. (ChoicePoint) paid $10 million in civil penalties and $5 million in consumer redress to settle the FTC's charges in 2006.[86] In a May 2005 filing with the Securities and Exchange Commission, BJ's estimated that these claims were worth approximately $13 million.[87] ChoicePoint also was involved in a second enforcement action in 2009, for violations of its 2006 consent order.[88] At the time BJ's Wholesale Club, Inc. settled the FTC's charges, banks and credit unions were pursuing BJ's to recover for fraudulent payments and for damages associated with the cancellation and re-issuance of credit and debit cards.[89] The FTC consent order against CardSystems Solutions—a third-party payment service provider charged with violations of FTC Act Section 5's unfair or deceptive acts or practices authority—provides a good example of its requirements for new comprehensive data security programs to protect the security, confidentiality, and integrity of personal information that it collects or receives from consumers by adopting administrative, technical, and

85. For a summary of FTC Section 5 enforcement actions involving financial privacy and data security, see Enforcement, FED. TRADE COMM'N, http://www.ftc.gov/privacy/privacy initiatives/promises_enf.html (last visited Nov. 21, 2010). For an example of an FTC settlement requiring implementation of a comprehensive information security program and long-term independent audits, see Settlement of Separate Actions, *supra* note 5.

86. Press Release, Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), http://www.ftc.gov/opa/2006/01/choicepoint.shtm. The violations of the Fair Credit Reporting Act included failure to employ reasonable procedures to screen prospective clients for its specialized credit reporting services and eventual disclosures of the personally identifiable information pertaining to more than 160,000 customers when the clients to whom disclosures were made had applications that raised red flags, including using commercial mail drops as business addresses, using cell phone numbers as business telephone contact numbers, and paying for services using money orders drawn on multiple issuers. *See* Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 5, 7, United States v. Choicepoint, Inc., No. 06-cv-0198 (N.D. Ga. Jan. 30, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf. The FTC also charged that ChoicePoint in one case continued to provide consumer information after ChoicePoint had suspended the customer for nonpayment on more than one occasion. *Id.* at 7.

87. Press Release, Fed. Trade Comm'n, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), http://www.ftc.gov/opa/2005/06/bjwholesale.shtm [hereinafter BJ's Wholesale Club Press Release].

88. *See* Supplemental Stipulated Judgment and Order for Permanent Injunction and Monetary Relief, United States v. ChoicePoint, Inc., No. 06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009), *available at* http://www.ftc.gov/os/caselist/choicepoint.shtm. ChoicePoint also is a recidivist like BP. *See id.*

89. *See* BJ's Wholesale Club Press Release, *supra* note 87. For the complaint and consent order, see *In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465 (2005).

physical safeguards for personally identifiable information.[90] Of course, design and implementation of a new security program is a significant expense.

II. INTERNATIONAL CONVENTION GOVERNING NOTICE OF AND COMPENSATION FOR MARITIME SPILLS OF OIL AND OTHER HAZARDOUS SUBSTANCES

As mentioned above, there may be many parallels drawn between payments data spills and pollution from maritime accidents. Both impose costs on unsuspecting people that include huge risks of collateral damage to livelihoods. Maritime accidents affect fisheries, shipping activities, and the welfare of shore life. Businesses affected by data spills may experience a fall in share values/market capitalization,[91] exclusion from participation in payment systems,[92] and reputational damage. Individuals may experience emotional distress, decreased credit ratings, and a loss of the privilege of using credit rather than cash.

Both types of spills impose costs from long-term remediation efforts. Indeed, reports suggest that TJX spent at least $256 million on recovery efforts related to its data spill and that its overall losses were $1 billion.[93] Exxon claims to have spent about $2 billion cleaning up the 11-million-gallon spill from the Exxon Valdez and another $1 billion to settle civil and criminal charges against it.[94] Consequential damage from the grounding to sea life alone included the loss of 250,000 seabirds and more than 20 orca whales.[95] To compensate victims affected by Deepwater Horizon, BP has established a fund in the range of $20 billion[96] and spent more than $3 billion on the early stages of the clean-up and recovery.[97] To deal with the

---

90. *In re* CardSystems Solutions, Inc., No. 052-3148, 2006 WL 515749 (F.T.C. Feb. 23, 2006). For more information about this and other FTC actions involving payments data security breaches, see Martha L. Arias, *Internet Law—Computer and Data Security Breaches*, INTERNET BUS. L. SERVS. (Sept. 17, 2007), https://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1852.

91. *See* Kimberly K. Peretti, *Data Breaches: What the Underground World of "Carding" Reveals*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 375 (2009).

92. *E.g.*, Anthony M. Freed, *Visa Puts Heartland on Probation Over Security Breach*, SEEKING ALPHA (Mar. 13, 2009), http://seekingalpha.com/article/125849-visa-puts-heartland-on-probation-over-security-breach (reporting the suspension of the Heartland system from VISA participation until it had been recertified).

93. Peretti, *supra* note 91, at 380; Kerber, *supra* note 83.

94. *See* Jonathan Stempel, *Special Report: BP Oil Spill a Gusher for Lawyers*, REUTERS, Jun. 30, 2010, *available at* http://www.reuters.com/article/idUSTRE65T2MZ20100630.

95. Dan Joling & Mark Thiessen, *In Alaska, Painful Memories of Exxon Valdez*, CBSNEWS.COM, May 3, 2010, http://www.cbsnews.com/stories/2010/05/03/national/main6456927.shtml.

96. Fiona Maharg-Bravo & Robert Cyran, *Tallying BP's Bill on the Gulf Coast*, N.Y. TIMES, July 14, 2010, at B2.

97. Jad Mouawad, *BP Begins Its Next Challenge: Reassuring Investors*, N.Y. TIMES, July 8, 2010, at B1.

consequences of these oil spills many conventions have been concluded. Importantly, these conventions serve as useful comparisons for ways to deal with data spills.

MARPOL 73/78 is the short-hand name for one such convention, the 1973 International Maritime Organization convention and a series of related amendments, annexes, and protocols, including the 1978 and 1997 amendments to the convention.[98] MARPOL 73/78 is not the only convention dealing with the consequences of maritime collisions or with certain forms of hazardous substance releases from sea-going ships.[99] There is also, for example, the Convention on Limitation of Liability for Maritime Claims.[100] U.S. laws also govern incidents such as fatalities and oil spills.[101]

MARPOL has features that could serve as a template for a regime to deal with data spills. It is a document with global force and, therefore, with legitimacy, and it relies on governmental mechanisms, non-governmental organizations, and—as one of its most attractive features for the purpose of addressing data spills provides—its scheme relies on a diverse group called "experts" to solve various technical, legal, and political problems that arise under its provisions.[102]

MARPOL 73/78, the amendments to the 1978 Protocol and subsequent regulations implementing the whole scheme, and U.S. laws implementing the MARPOL scheme or other environmental protection requirements offer four guiding points for a possible framework for payments data spills: (1) the requirement of compulsory notice to a central agency;[103] (2) a compensation scheme that extends to third-parties affected by the hazardous substance spills;[104] (3) operational restrictions;[105] and (4) the requirement to outfit sea-going ships with double hulls or other alternative protections, such as double bottoms, so as to protect against the accidental release of

---

98. *International Convention for the Prevention of Pollution from Ships (MARPOL)*, INT'L MARITIME ORG., http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-(MARPOL).aspx (last visited Dec. 27, 2010).

99. *E.g.*, International Convention for the Prevention of Pollution of the Sea by Oil, concluded May 12, 1954, 12 U.S.T. 2989, T.I.A.S. No. 4900, 327 U.N.T.S. 3 [hereinafter OilPOL]; International Convention on Civil Liability for Oil Pollution Damage, *concluded* Nov. 29, 1969, 973 U.N.T.S. 3, amended by Protocol, Nov. 27, 1992, 1956 U.N.T.S. 255.

100. Convention on Limitation of Liability for Maritime Claims, *concluded* Nov. 19, 1976, 1456 U.N.T.S. 221.

101. Death on the High Seas Act of 1920, 46 U.S.C. §§ 30302–30308 (2006); Federal Water Pollution Control Act (Clean Water Act), 33 U.S.C. §§ 1251–1321 (2006).

102. *See* Clay Maitland, *Is MARPOL Dead?*, MARINE LOG, Dec. 2007, at 52 (concluding that MARPOL is not dead).

103. *See* MARPOL 73/78, *supra* note 11, at art. 8, ¶ 2(b). The 1972 Federal Water Pollution Control Act (Clean Water Act) requires notice of spills of hazardous substances, such as oil. 33 U.S.C. § 1321(b)(5).

104. MARPOL 73/78, *supra* note 11, at art. 7, ¶ 2.

105. Amendments to the Annex of the Protocol of 1978 Relating to the International Convention for the Prevention of Pollution From Ships, 1973, Resolution MEPC.117(52), *adopted* Oct. 15, 2004, 2057 U.N.T.S. 68 [hereinafter Revised Annex 1 of MARPOL 73/78].

hazardous substances in the ships.[106] A fifth guiding principle of the oil spill prevention scheme—the creation of the International Maritime Organization (IMO) as an international organization focused on the problem—predated MARPOL.[107]

A comprehensive national or international approach to data security breaches might even avoid one of the pitfalls that MARPOL and other international conventions and U.S. environmental protection statutes share in terms of fixed liability limits that prove very hard to update. For example, the liability limit in the Clean Water Act was intended to subject violators to civil penalties in amounts "up to $25,000 per day of violation or an amount up to $1,000 per barrel of oil."[108]

But regardless of these imperfections, the five pivot points found in MARPOL, its amendments and IMO regulations as well as U.S. environmental protection laws offer some useful approaches for data security spills.

A. COMPULSORY NOTICE OF SPILLS

One of the most useful analogies that payments data security can draw from MARPOL 73/78 is its requirement of compulsory notice of oil spills to a central agency.[109] There is no *de minimus* rule in the MARPOL scheme; that is, the ship's operators must report every spill or discharge.[110]

In contrast, enacted state legislation and pending federal bills regarding data security breaches, discussed *infra*, only require prompt notice to law enforcement if the breach affects a threshold number of individuals or records—such as at least 10,000 individuals or a million or more records, and separate notices to consumers whose card data has been breached.[111] It

---

106. *Id.* at regulation 19.

107. *See Introduction to IMO*, INT'L MARITIME ORG., http://www.imo.org/About/Pages/Default.aspx (last visited Dec. 28, 2010) (describing the IMO's origins in 1948 as the Inter-Governmental Maritime Consultative Organizations, a name changed to International Maritime Organization in 1982). The IMO entered into force in 1958 just prior to the entry into force of OilPOL. *Marine Environment Pollution Prevention Background*, INT'L MARITIME ORG., http://www.imo.org/OurWork/Environment/PollutionPrevention/OilPollution/Pages/Background.aspx (last visited Dec. 28, 2010).

108. 33 U.S.C. § 1321(b)(7)(A) (2006).

109. *See* MARPOL 73/78, *supra* note 11, at art. 8; Revised Annex I of MARPOL 73/78, *supra* note 105, at regulation 37.

110. *See* MARPOL 73/78, *supra* note 11, at art. 8; Revised Annex I of MARPOL 73/78, *supra* note 105, at regulation 37.

111. Nearly every federal data security bill allows delays in notices to consumers so that law enforcement investigations may take place. *E.g.*, Data Accountability and Trust Act, H.R. 2221, 111th Cong. § 3(c)(2) (as passed by House, Dec. 8, 2009) (providing delay for regular law enforcement purposes and for longer periods if notification would threaten national or homeland security). In both cases, delays must be based on determinations of necessity, and requests for delays are made in writing. *E.g.*, Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. § 311(d) (2009). Additional delays may be requested. *E.g.*, H.R. 2221, § 3(c)(2)(A) (thirty days original delay for general law enforcement purposes subject to subsequent requests for delay with no specified outer limit if requests also made in writing).

is this Article's position that, in order to protect critical infrastructure assets and national security, notice between the entity that suffers the breach and a central authority (at least at the national level) that a payments data spill has occurred should be mandatory regardless of its size, rather than based on some threshold. Proprietary payments systems rules and credit and debit card master agreements should require the merchants, payments processors, or financial institutions whose systems are breached to notify their counterparties as well, regardless of the number of records or accounts affected. Thresholds, I would argue, keep from central scrutiny data problems at their beginning, may allow them to spread, and certainly provide no early-warning system equivalent of orchestrated attacks on a retailer, payment system, or financial institution that would protect everyone involved.

B. COMPENSATION FOR THIRD-PARTY LOSSES

MARPOL 73/78 is also part of a longstanding scheme of compensation for third-party losses that reaches back to 1954, beginning with the convention known as OilPOL.[112] Compensation allows affected communities and individuals to survive the damage to livelihoods and to physical environments on which they depend or around which they live. Since OilPOL, various international conventions and domestic laws implementing them in some cases have increased the amount of first-level compensation.[113]

The group of international conventions providing for compensation includes two that predate MARPOL 73/78, the 1969 International Convention on Civil Liability for Oil Pollution Damage (commonly known as the 1969 Civil Liability Convention), and the 1971 International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage (commonly known as the 1971 Fund Convention), each of which has been replaced by new protocols in 1992, now known, respectively, as the 1992 Civil Liability Convention and the 1992 Fund Convention.[114] The 1992 Civil Liability Convention imposes

---

112. OilPOL, *supra* note 99. The 1978 Protocol to the 1973 Convention essentially replaced OilPol. *See Background on Pollution Prevention and MARPOL 73/78*, *supra* note 11. However, Congress then repealed the Oil Pollution Act of 1961, Pub. L. No. 87-167, 75 Stat. 402, which had implemented OilPOL and the Oil Pollution Act Amendments of 1973. Act to Prevent Pollution from Ships of 1980, Pub. L. No. 96-478, 94 Stat. 2303 (codified as amended at 33 U.S.C. §§ 1901–1915).

113. U.S. statutes implemented these compensation schemes to include, *inter alia,* Federal Water Pollution Control Act (Clean Water Act), 33 U.S.C. §§ 1251–1321 (2006), the Outer Continental Shelf Lands Act Amendments of 1978, 43 U.S.C. § 1814 (1988) (repealed 1990), the Trans-Alaska Pipeline Authorization Act, 43 U.S.C. § 1653 (1988), and the Deepwater Port Act, 33 U.S.C. § 1517 (1988).

114. *The International Regime for Compensation for Oil Pollution Damage: Explanatory Note Prepared by the Secreteriat of the International Oil Pollution Compensation Funds*, INT'L OIL POLLUTION COMPENSATION FUNDS (Dec. 2010), http://www.iopcfund.org/npdf/genE.pdf [hereinafter Explanatory Note].

strict liability on ship owners for oil pollution damage.[115] The 1992 Fund Convention provides supplementary compensation for oil pollution victims if the former convention's compensation is inadequate.[116] In addition, a Protocol to the 1992 Fund Convention created a third tier compensation prospect through the International Oil Pollution Compensation Supplementary Fund, raising the maximum payable for one incident to 750,000,000 Special Drawing Rights, which is equivalent to $147,500,000.[117]

Examples of domestic legislation providing for compensation exist in the United States and Turkey. In the United States, the OPA specifies the types of damages that individuals and other entities that suffered injury could obtain from persons responsible for oil spills.[118] These include damages to natural resources, real or personal property, subsistence uses of natural resources, revenues, public services, and profits.[119] In addition, it specifies the scope of clean-up costs for which responsible persons are liable, including containment and actions necessary to "minimize or mitigate damage to public health or welfare, including, but not limited to, fish, shellfish, wildlife, and public and private property, shorelines, and beaches[.]"[120] The OPA allows the States to impose liability on responsible parties beyond the liability that the Act provides.[121] Turkey's law was adopted in 2005.[122]

A special scheme for damages to third-parties—like the overall scheme supporting compensation for oil-spill victims briefly described above—might be used to sustain credit reporting blocks or monitoring and recovery expenses, particularly when breaches affect smaller merchants or institutions, or other sorts of damages that are hard to quantify in advance.

---

115. *See id.*; *see also* International Convention on Civil Liability for Oil Pollution Damage, 1992, art. 1 ¶ 6, art. 3 ¶ 1, *opened for signature* Jan. 15, 1993, 1956 U.N.T.S. 255, *available at* http://www.iopcfund.org/npdf/Conventions%20English.pdf.

116. *See* Explanatory Note, *supra* note 114; *see also* International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage, 1992, at art. II, ¶ 1, *opened for signature* Jan. 15, 1993, 1953 U.N.T.S. 330, *available at* http://www.iopcfund.org/npdf/Conventions%20English.pdf.

117. Explanatory Note, *supra* note 114. To determine the daily value of Special Drawing rights under this scheme, see *Exchange Rate Archives by Month*, INT'L MONETARY FUND, http://www.imf.org/external/np/fin/data/param_rms_mth.aspx (last visited Dec. 28, 2010). For a comprehensive analysis of the overall oil pollution damages scheme, see MICHAEL MASON, TRANSNATIONAL COMPENSATION FOR OIL POLLUTION DAMAGE: EXAMINING CHANGING SPATIALITIES OF ENVIRONMENTAL LIABILITY (2002), http://eprints.lse.ac.uk/570/1/RPESA-no69(2002).pdf.

118. Oil Pollution Act of 1990, 33 U.S.C. §§ 2701–2720, 2731–2738 (2006).

119. *Id.* § 2702(b)(2)

120. *Id.* § 2701(30).

121. *Id.* § 2718(a).

122. For a thorough discussion of this law, see MURAT TURAN, TURKEY'S OIL SPILL RESPONSE POLICY: INFLUENCES AND IMPLEMENTATION (2009), *available at* http://www.un.org/Depts/los/nippon/unnff_programme_home/fellows_pages/fellows_papers/turan_0809_turkey.pdf.

In establishing a compensation scheme for counter-party and consumer damages from data spills, however, we should take care to create a mechanism to provide for periodic increases in basis compensation. This would avoid the problems associated with compensation schemes in which allowed damages have not kept pace with inflation, such as in the Death on the High Seas Act of 1920[123] or in 13 U.S.C. § 1321(7)(A), which establishes a civil penalty for "owner[s], operator[s] or person[s] in charge of any vessel, onshore facility or offshore facility from which oil or a hazardous substance is discharged in violation of" 13 U.S.C. § 1321(3) that is capped at $25,000 per day of violation for discharges of oil or other hazardous substances or at up to $1,000 per barrel of oil or unit of reportable quantity of hazardous substances discharged.[124] In addition, in cases in which the violation "was the result of gross negligence or willful misconduct" of an owner, operator, or person in charge described in 13 U.S.C. § 1321(7)(A), the person is "subject to a civil penalty of not less than $100,000, and not more than $3,000 per barrel of oil unit of reportable quantity of hazardous substance discharged."[125]

In addition, the compensation scheme might reward prompt and accurate reporting of the data spill to avoid the obvious temptation to lowball the estimate of damages inflicted. In the Deepwater Horizon incident, for example, there were many reports that BP was under-reporting the discharge from the well so that it could take advantage of the "strict liability" penalties in 13 U.S.C. § 1321(7)(A) and avoid the higher penalties for "gross negligence" provided in 13 U.S.C. § 1321(7(D).[126]

C. OPERATIONAL RESTRICTIONS

MARPOL 73/78 imposes additional operational requirements and some restrictions on tankers and other vessels that do not meet its mandates. For example, just as VISA suspended RBS PayCard's approved service provider status after its breach revealed that its compliance with PCI DSS was inadequate,[127] vessels that do not meet certain criteria under MARPOL may not enter certain waters or ports,[128] and may be required to keep expanded records and undergo additional inspections.[129]

This multi-pronged approach to prevention may be more effective than the single-factor reliance on encryption or double-factor encryption and best

123. Death on the High Seas Act of 1920, 46 U.S.C. §§ 30302–30308 (2006).
124. Clean Water Act, 33 U.S.C. § 1321(7)(A) (2006).
125. *Id.* § 1321(7)(D).
126. John Schwartz, *Liability at Issue in Oil Flow Rate in Gulf*, N.Y. TIMES, Jul 19, 2010, at A17; *see also* Press Release, The Select Committee on Energy, Independence and Global Warming, Markey: Flow Rate Report Shines Light on BP's Financial Liability, True Size of Spill (May 27, 2010), http://globalwarming.house.gov/mediacenter/pressreleases_2008?id=0255.
127. Ashford, *supra* note 70.
128. Revised Annex I of MARPOL 73/78, *supra* note 105, at regulations 20–21.
129. Revised Annex I of MARPOL 73/78, *supra* note 105.

practices approaches seen in state data security breach laws as well as pending federal legislation.[130]

D. DOUBLE HULLS AND COMPARABLE SAFE-DESIGN REQUIREMENTS

MARPOL 73/78 also requires specific structural defenses to guard against oil spills and other discharges into the sea. For tankers built after 1981, MARPOL requires that construction be double-hulled.[131] The convention requires that vessels with large capacities but built before June 1, 1982 or contracted to be built before that year, be retrofitted with double bottoms and structural improvements to their sides.[132] Vessels without appropriate structural defenses as required by MARPOL should not expect access to certain ports.[133] Similarly, payments systems participants that cannot comply with PCI DSS's required firewalls and 128-bit encryption security features—or that employ EMV/chip-and-PIN technology instead—might be precluded or suspended from certain payments systems. Such was the fate of Heartland after its breach.[134]

E. MODEL FOR INTERNATIONAL COOPERATION AND AVOIDANCE OF TRADE-HINDERING NATIONAL LEGISLATION

The fifth lesson that MARPOL 73/78 offers to the solution of payments data spills relates to its role as a model for international cooperation in the effort to reduce the temptation to deal with certain issues piecemeal through national legislation. Because of rising evidence that the perpetrators of data security breaches operate internationally,[135] and because the threat of transnational criminal prosecution may not deter cyber thieves, international cooperation through private standard setting and international conventions

---

130. *See infra* Part IV.

131. Revised Annex I of MARPOL 73/78, *supra* note 105, at regulation 20.

132. *Id.*

133. *Id.* For an analogous situation regarding data breaches, see Ashford, *supra* note 70 (describing how banks may be removed from Visa's and Mastercard's list of validated service providers if they are not compliant with the Payment Card Industry Data Security Standard).

134. *E.g.*, Freed, *supra* note 92 (reporting the suspension of the Heartland system from VISA participation until it had been recertified); Lemos, *supra* note 66 (mentioning the use of low-level thieves called "cashers" to withdraw funds from ATMs in Montreal, Moscow, Hong Kong, and other cities in the U.S. and abroad depleting 100 accounts and revealing personal information on 1.5 million cardholders and the social security numbers of 1.1 million of them); Robert McMillan, *FTC Says Scammers Stole Millions, Using Virtual Companies,* COMPUTER WORLD, Jun. 27, 2010, http://www.computerworld.com/s/article/9178560/FTC_says_scammers_stole_millions_using_virtual_companies (scammers used U.S. residents to move money to Bulgaria, Cyprus, and Estonia) [hereinafter McMillan, *FTC Catches Scammers*]. More recently, reports suggest that Russian hackers broke into check image depositary and used information to generate counterfeit checks and stole $9 million. Elinor Mills, *Check Counterfeiting Using Botnets and Money Mules*, CNET NEWS (July 28, 2010), http://news.cnet.com/8301-27080_3-200111885-245.html.

135. *See, e.g.*, McMillan, *FTC Catches Scammers*, *supra* note 134.

offers an attractive approach for the prevention and resolution of data security incidents.

III. HOW DO PAYMENTS DATA SPILLS AND MARITIME SPILLS COMPARE?

Part II of this Article focuses on costs associated with the prevention and remediation of spills, both payments data and oil-related. This Part focuses on the causes of spills. In this regard, payments data spills and maritime accidents share things in common. First, both may derive from insiders' *negligence or recklessness,* or *cost-cutting that affects risk-prevention measures*.[136] Examples of negligence leading to data spills include:

- Theft of unencrypted information on hard drives stored in an apparently unsecure closet in a training facility of BlueCross BlueShield of Tennessee. These hard drives contained data, as well as photos of the screens on which trainees and operators were working that revealed sensitive personally identifiable information about customers;[137] and
- The spectacular TJX breach affecting 94 million payment records of credit cards and debit cards involving the use of wireless Internet transmissions of data vulnerable to interception in a process known as "war driving" in which thieves use readers to capture transmissions leaving known store locations.[138]

Maritime examples include:

- The disarming of one or more warning systems on the Deepwater Horizon oil drilling platform in the days and weeks prior to the explosion and spill, and the failure to heed other signals that important safety features were not functioning as planned;[139]
- The grounding of the Exxon Valdez in the Valdez Inlet near Anchorage, Alaska in 1989. Investigation of the cause of the accident revealed that, despite the known shoal dangers of Prince William Sound through which the Valdez was moving,[140] only one officer was on the bridge at the time of the accident and that the

136. For a discussion on oil spills, see Achenbach & Hilzenrath, *supra* note 39.

137. *See* McMillan, *Data Theft*, *supra* note 35.

138. Byron Acohido, *Cyberthieves Find Workplace Networks are Easy Pickings; Simple Hacking Techniques Have Potential to Collect Data From Any Entity Using a Digital Network,* USA TODAY, Oct. 9, 2009, at B1 (discussing the TJX and Hannaford data security breaches and the means used to intercept data).

139. David S. Hilzenrath, *Alarm System on Rig Was Disabled, Technician Testifies*, WASH. POST, July 24, 2010, at A5.

140. *See* ALASKA OIL SPILL COMMISSION, *supra* note 38.

pilot had been under the influence of alcohol at the time of the grounding;[141] and

- The Cosco Busan accident that spilled 53,569 gallons of heavy crude into San Francisco Bay on November 7, 2007.[142] The United States filed felony and misdemeanor charges against the Cosco Busan's management and pilot for sailing in fog, travelling at an unsafe speed, failing to make plans or use radar, and falsifying documents.[143]

Second, the sources of spills may be entirely different. For example, the 1978 wreck of the Amoco Cadiz was caused by the failure of the tanker's steering mechanism and subsequent rough weather, which in turn caused the tanker to split apart, spilling 68.4 million gallons of oil and despoiling more than 125 miles of the coast of France.[144] This tanker was not fitted with a double hull—because MARPOL's requirement was not in effect at the time—placing its cargo at greater risk in the event of grounding.[145]

Does the grounding of the Exxon Valdez bear a stronger resemblance to the BlueCross BlueShield of Tennessee spill—which involved unencrypted data in an unguarded location—or the Google spill—which involved the high-tech penetrations of significant firewalls around wire transfer systems?[146]

While considering the above, it may be helpful to think about the differences between navigating correctly charted waters, on the one hand, and navigating areas in which recent storms or sand accretions may affect the reliability of the charts. Or, in other words, navigating around known rocks is easier because, normally, *big rocks do not move often and sand does*.[147] The chart and, therefore, the charted course should be all right if all one is interested in is avoiding the rocks. But the same won't work with sand, which is constantly eroding and accreting.[148]

---

141. Stephens, *supra* note 3; *see also* ALASKA OIL SPILL COMMISSION, *supra* note 38, at 27. Among other sea and shore life, the oil spill killed 250,000 sea birds and more than twenty orca whales in Prince William Sound, Alaska, alone. Joling & Thiessen *supra*, note 95.

142. UNITED STATES DEPARTMENT OF HOMELAND SECURITY, INCIDENT SPECIFIC PREPAREDNESS REVIEW (ISPR) M/V *COSCO BUSAN* OIL SPILL IN SAN FRANCISCO BAY: REPORT ON INITIAL RESPONSE PHASE (2008), *available at* http://www.uscg.mil/foia/CoscoBuscan/Cosco BusanISPRFinalx.pdf (listing number of birds caught (1,039), cleaned (681), and dead (1,365) due to the Cosco Butan oil spill and discussing origins of the spill).

143. Bob Egelko, *Felony Charges for Ship's Management*, S. F. CHRON., July 24, 2008, at B3.

144. Allen Tony, *MV Amoco Cadiz*, THE WRECKSITE ARCHIVE (June 26, 2007), http://www.wrecksite.eu/wreck.aspx?10339.

145. *See* Background on Pollution Prevention and MARPOL 73/78, *supra* note 11.

146. *More E-Mail Account Details Leak Online*, N.Y. TIMES GADGETWISE BLOG (Oct. 6, 2009, 11:05 PM), http://gadgetwise.blogs.nytimes.com/2009/10/06/more-e-mail-account-details-leaked-online/?scp=3&sq=wire%20transfer&st=cse.

147. Interview with Roland Trope, Esq., Partner, Trope & Schramm, LLP, in Coral Gables, FL (Jan. 25, 2010).

148. Examples of accretions and erosion abound. Storms may cause breaches that radically alter tidal flows in their vicinities and lesser weather changes may cause significant shifts in sand bars

But, as new operating systems are rushed to market, data security confronts efforts by cyber-thieves that are analogous to movements of both rocks and sand on a constant basis as thieves search for any available vulnerability and seek to penetrate systems that may have been considered impenetrable just prior to the breach. So, in some respects, detecting and preventing risks to data security may be harder than avoiding the aforementioned types of shipping accidents. However, the risks to critical infrastructures and national security are such that stronger incentives for appropriate levels of monitoring and deterrence as well as some legal, centralized, or collective solutions are needed.

IV. LEGISLATIVE RESPONSES TO DATA SPILLS AND PROSPECTS—DO PROPOSALS SUFFICIENTLY ADDRESS SPILL PREVENTION AND DATA SPILL REMEDIES FOR BUSINESSES OR CONSUMERS WHOSE SYSTEMS OR PERSONAL INFORMATION IS BREACHED?

A. CONGRESSIONAL LEGISLATION

Notwithstanding the numerous data spills and the damages resulting from them, the only recent federal law specifically related to data breach notification is the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act).[149] The Act expanded the enforcement jurisdiction of the Health Insurance Portability and Accountability Act (HIPAA)[150] to allow state attorneys to enforce HIPAA's provisions and implementing regulations.[151]

---

and shoals that affect tides or otherwise threaten maritime safety. *See, e.g.*, Nelson Sigelman, *Three Years Later, Norton Point Breach Marches On*, MARTHA'S VINEYARD TIMES, Apr. 29, 2010, http://www.mvtimes.com/marthas-vineyard/article.php?id=536; Nelson Sigelman, *Ocean Forces Continue to Shape Katama Cut*, MARTHA'S VINEYARD TIMES, June 19, 2008, http://www.mvtimes.com/2008/06/19/news/norton-point-breach.php. Studies of sand-bar migration include Edith L. Gallagher, Steve Elgar & R.T. Guza, *Nearshore Sandbar Migration*, 106 J. GEOPHYSICAL RES. 11,623 (2001); Edith L. Gallagher, Steve Elgar & R.T. Guza, *Observations of Sand Bar Evolution on a Natural Beach*, 103 J. GEOPHYSICAL RES. 3203 (1998); D.J. Phillips & S.T. Mead, *Investigation of a Large Sandbar at Raglan, New Zealand: Project Overview and Preliminary Results*, 1 REEF J. 267 (2009).

149. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 115, 226 (2009) (codified in scattered sections of 42 U.S.C.).

150. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 16, 26, 29, 42 U.S.C.).

151. Health Information Technology for Economic and Clinical Health Act § 13410(e). Using this new authority, the State of Connecticut was reported to be investigating the WellPoint data breach. *See* Joseph Goedert, *Conn. AG Probes WellPoint Breach,* HEALTH DATA MGMT (July 6, 2010), http://www.healthdatamanagement.com/news/breach-wellpoint-anthem-connecticut-attorney-general-40596-1.html. Prior to the HITECH Act, only the Secretary of Health and Human Services could enforce HIPAA's privacy and security rules. *See* Priscilla M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103, 1111 n.47 (2009) (citing GINA STEVENS & EDWARD C. LIU, CONG.. RESEARCH SERV., R40546, THE

Congress has been considering additional data security legislation since at least 2005.[152] Thus far in the 111th Congress, the House has passed two bills—the Data Accountability and Trust Act[153] and the Cybersecurity Enhancement Act of 2010.[154] This section looks at those bills, and two Senate bills introduced in the 111th Congress, to consider whether their provisions would help or hinder the deterrence and resolution of payments data spills. It also discusses H.R. 1319, the Informed P2P User Act, and S. 3027, a companion bill to H.R. 1319, which was introduced in the Senate in February 2010.

Each of these bills would impose new requirements on the handling of financial account data that is among the most valuable data for data thieves to access. Each bill only attempts to address a segment of a total data security scheme. For example, the Data Accountability and Trust Act directs the Federal Trade Commission to promulgate regulations to require owners and possessors of electronic data containing personal information and engaged in interstate commerce to provide for security procedures, vulnerability testing, and proper disposal of data, and requires notification of data security breaches to the FTC and to affected individuals.[155] The Cybersecurity Enhancement Act focuses on the creation of strategic plans and support for research in the data security field, and requires the National Science Foundation to recruit for and fund a scholarship program for professionals in this field.[156]

As a result, merchants, payments processors, and operators of payments systems will be subject to the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA) and the Fair and Accurate Transactions Act (FACTA) requirements, and "data brokers" may be subject to new statutes such as the Data Accountability and Trust Act.[157] Of course, providers of consumer financial services and products are already governed

---

PRIVACY AND SECURITY PROVISIONS FOR HEATH INFORMATION IN THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009, at 18 (2009)).

152. Beginning in the 109th Congress to early March 2010, numerous bills dealing with data security from different perspectives have been introduced in the House of Representatives. *See generally* Legislation in Current Congress, LIBRARY OF CONGRESS, www.thomas.gov (last visited Dec. 28, 2010). Among these were Consumer Notification and Financial Data Protection Act of 2005, H.B. 3374, 109th Cong. (2005) and the Consumer Data Security and Notification Act of 2005, H.B. 3140, 109th Cong. (2005), from the Committees on Banking and Financial Services and on the Judiciary, respectively. For an excellent history of Congress' interest in breach notification legislation, see Regan, *supra* note 151, at 1112.

153. Data Accountability and Trust Act, H.R. 2221, 111th Cong. (as passed by House, Dec. 8, 2009).

154. Cybersecurity Enhancement Act of 2010, H.R. 4061, 111th Cong. (as passed by House, Feb. 9, 2010).

155. H.R. 2221 §§ 2–3.

156. H.R. 4061 §§ 103, 106.

157. *See* Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003) (codified as amended at 15 U.S.C. § 1601).

by Title V of the GLBA.[158] S. 1490 creates enforcement mechanisms for violations of its own requirements,[159] and it authorizes the FTC to promulgate regulations to implement its privacy and data security requirements.[160] In addition, the Senate bill confirms the role of the United States Secret Service as the primary federal agency to be notified of data security breaches[161] and strengthens the tools that the federal government may use in combating such breaches.[162] It does not expand remedies for consumers, largely because error resolution for unauthorized transactions should be covered by rights available to them under laws governing other payments system rules including the Fair Credit Billing Act[163] for credit card transactions or the Electronic Fund Transfer Act for debit and payroll card transactions.[164] However, it leaves consumers affected by data spills affecting bank and other transaction accounts, including gift cards, without a specific remedy.

1. Bills Passed by the House of Representatives

The House of Representatives has passed two data security bills since the beginning of 2009. These bills are:

a. H.R. 1319

The House of Representatives passed H.R. 1319 on December 8, 2009; it requires P2P providers to disclose to users which files a P2P program can share and consent of the users before the files can be shared over that program.[165] The bill also makes it unlawful for any entity covered by its provisions to prevent an owner or authorized user of a protected computer

158. Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. § 301 (as reported by S. Comm., Nov. 5, 2009) (exempting financial institutions regulated under GLBA from S. 1490). S. 1490 also would not apply to entities governed by HIPAA. *Id.* (exempting HIPAA-regulated entities from S. 1490).

159. *Id.* § 101 ("Organized criminal activity in connection with unauthorized access to personally identifiable information"); *id.* § 102 ("Concealment of security breaches involving sensitive personally identifiable information"); *id.* § 104 ("Effects of identity theft on bankruptcy proceedings"); *id.* § 202 (FTC enforcement powers against data brokers); *id.* § 303 (FTC enforcement of requirements for privacy and security of personally identifiable information programs); *id.* §§ 317–18 (enforcement by state and federal Attorney Generals of breach notification requirements).

160. *Id.* § 202.

161. *Id.* § 316.

162. *Id.* §§ 101–02, 202, 302, 317, 318.

163. Fair Credit Billing Act of 1974, Pub. L. No. 93-495, §§ 301–08, 88 Stat. 1500 (codified as amended in scattered sections of 15 U.S.C.).

164. Electronic Fund Transfer Act, Pub. L. No. 95-630, § 2001, 92 Stat. 3728 (codified at 15 U.S.C. §§ 1693–1693r (2006)).

165. Informed P2P User Act, H.R. 1319, 111th Cong. (2009). Section 2's requirement of notice prior to installation or downloading of a P2P program or activation of a file-sharing function of such a program does not apply to pre-installed software or to software upgrades. *Id.* § 2(a)(2) ("Non-application to pre-installed software"); *id.* § 2(a)(3) ("Non-application to software upgrades").

from: (1) using "reasonable efforts" to block installation of a file-sharing program or function if covered by the bill; and (2) "having a reasonable means to" disable covered file-sharing programs or removing file-sharing programs that the covered entity caused to be installed or induced another person to install.[166] The bill grants authority to the FTC to enforce its requirements making failure of the provider to comply the equivalent of a violation of a rule defining unfair or deceptive acts or practices under § 18(a)(1)(B) of the FTC Act.[167] The bill also authorizes the FTC to promulgate rules to accomplish its provisions.[168]

b. H.R. 2221—The Data Accountability and Trust Act

Section 2 of the Data Accountability and Trust Act instructs the FTC to promulgate regulations to:

> [R]equire each person engaged in interstate commerce that owns or possesses data containing personal information, or contracts to have any third party entity maintain such data for such person, to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information taking into consideration—
>
> (A) the size of, and the nature, scope, and complexity of the activities engaged in by, such person;
>
> (B) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and
>
> (C) the cost of implementing such safeguards.[169]

One of the problems with H.R. 2221 is its safe harbor from liability for encrypted data because encryption alone[170] is unlikely to sufficiently protect data from all hacking. Rather, it is the bundle of physical, administrative, and technical safeguards—which include but are not limited to encryption efforts—that are more likely to yield comprehensive protections. The incident at BlueCross BlueShield of Tennessee discussed *supra* demonstrates how easily data may be stolen, particularly in large quantities, if more than one of the three forms of protection is not in use.

With the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 in July 2010, it is unclear whether the rulemaking authority that H.R. 2221 granted to the FTC will remain there

166. *Id.* § 2(b).
167. *Id.* § 3.
168. *Id.* § 5.
169. Data Accountability and Trust Act, H.R. 2221, 111th Cong. § 2(a)(1) (as passed by House, Dec. 8, 2009).
170. *Id.* § 3(f)(2)(A).

or will transfer to the newly created Bureau of Consumer Financial Protection.[171]

c. The Cybersecurity Enhancement Act of 2010, H.R. 4061

On February 4, 2010, the House of Representatives passed the Cybersecurity Enhancement Act of 2010. The Act, among other things, encourages social and behavioral research in cybersecurity,[172] provides for sponsorship of the development of scholarship and funding for training,[173] and encourages development and promotion of international cybersecurity technical standards and an "identity management research and development program."[174] If enacted, this bill is likely to encourage, in many respects, new approaches to deterrence and more cooperation on spill prevention.

2. Bills Considered by the Senate

The Senate has considered numerous bills since January, 2009. The following sections consider them in detail.

a. S. 1490—The Personal Data Privacy and Security Act of 2009

The Senate Committee on the Judiciary found that 9,300,000 individual records pertaining to personal payment transactions were compromised in 2008.[175] Based on this finding, the Committee reported out S. 1490, the Personal Data Privacy and Security Act of 2009. Its provisions cover consumer access and correction rights to information held about them by "data brokers."[176] Data brokers are entities that collect and sell commercial data, including personally identifiable information, to others, including governments.[177] This bill resolves gaps left between the GLBA and FACTA safeguards and disposal rules[178]—and indeed by HIPAA[179]—because entities already subject to those statutes and regulations would not be

171. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

172. Cybersecurity Enhancement Act of 2010, H.R. 4061, 111th Cong. § 104 (as passed by House, Feb. 4, 2010).

173. *Id.* § 106 ("Federal Cyber Scholarship for Service Program"); *id.* § 107 (requiring an analysis of and recommendations for securing an "adequate, well-trained Federal cybersecurity workforce").

174. *Id.* § 202 (development and promotion of "International Cybersecurity Technical Standards"); *id.* § 204 ("Identity Management Research and Development" program).

175. Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. § 2 (as reported by S. Comm., Nov. 5, 2009).

176. *Id.* §§ 201–04.

177. *Id.* § 3(5) (defining "data broker").

178. Disposal of Consumer Report Information and Records, 16 C.F.R. 682 (2006). This rule implements provisions of the Fair Credit Reporting Act. *See* 15 U.S.C. § 1681w (2006).

179. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 16, 26, 29, 42 U.S.C.).

governed by S. 1490.[180] Three key features of the bill require data brokers who collect or maintain records pertaining to 10,000 or more individuals to: (1) have privacy and security programs;[181] (2) audit and update those programs;[182] and (3) notify the United States Secret Service in the event of data security breaches if the number of individuals whose personal information is obtained without authorization exceeds 10,000 or if a database or network containing 1 million or more individual records is breached.[183] A separate requirement to notify individuals whose personally identifiable information is involved in the breach is excused if the data broker's risk assessment pertaining to that breach concludes that:

> (A) there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the *encryption of such information establishing a presumption that no significant risk exists*, or
>
> (B) there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the rendering of such sensitive personally identifiable information indecipherable through the use of best practices or methods, such as redaction, access controls, or other such mechanisms, which are widely accepted as an effective industry practice, or an effective industry standard, *establishing a presumption that no significant risk exists*[.][184]

b. S. 139—The Data Breach Notification Act

S. 139, the Data Breach Notification Act, is a narrower bill than S. 1490. It does not impose the same requirements for new privacy and security programs that S. 1490 imposes and its requirements for notification of individuals by "data brokers" after a data breach also are narrower.[185] S.

---

180. S. 1490.

181. *Id.* § 302.

182. *Id.* § 302(e).

183. *Id.* § 316. Notice to the U.S. Secret Service by entities experiencing data security breaches is limited to cases in which 10,000 individual victims may be involved or to cases in which a database or network is involved that contains information about one million individuals or more. *Id.*

184. *Id.* § 312(b)(1) (emphasis added).

185. S. 139's Sections 5 and 6 use a threshold for notices required to cases involving 5,000 or more individuals. Data Breach Notification Act, S. 139, 111th Cong. §§ 5–6 (2009); *see also id.* § 3(b)–(c) (safe harbor presumptions). However, Section 7 is similar to S. 1490 in that it requires notice to law enforcement only if the Serial Peripheral Interface Bus (SPI) of about 5,000 or more individuals is believed to have been acquired or the affected database or integrated databases contain SPI for one million or more individuals. *See id.* § 7.

For S. 1490, Title II's provisions on notice to affected consumers in Sections 311 and 312 do not contain the threshold that Sections 5 and 6 of S. 139 do. *See id.* §§ 311–12. Title III's Section 316 contains similar threshold to S. 139's Section 7 on notice to law enforcement—a key weakness in both bills. *See id.* § 316. However, Title III's Section 302 contains much stronger

139 allows a complete defense to liability in enforcement actions brought for violations of its requirements if the data is encrypted or the database follows "best practices."[186]

c. S. 773—The Cybersecurity Act

S. 773, the Cybersecurity Act of 2009, takes a very different approach from the other bills discussed in this part of the Article. It focuses on the development by the National Institute of Standards and Technology (NIST) of standards for federal government agencies', government contractors', and grantees' "critical infrastructure information systems and networks."[187] It also envisions financial assistance to create and support regional cybersecurity centers to assist small and medium-sized businesses.[188] Among many other provisions, it also places NIST in the position of representing the United States in international cybersecurity standards development projects,[189] makes the Department of Commerce (Commerce) the clearinghouse for all "cybersecurity threat and vulnerability information,"[190] and grants the Secretary access to data regardless of "any provision of law, regulation, rule or policy restricting such access."[191] The bill also authorizes the President to declare a "cybersecurity emergency" and to "'order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network.'"[192]

---

provisions on the scope, design, assessment of and periodic reassessment of protocols designed to protect SPI, and also on training of personnel to protect SPI. *Id.* § 302.

186. *See* S. 139 § 3(b)(2)(A)–(B).

187. Cybersecurity Act of 2009, S. 773, 111th Cong. § 6 (2009).

188. *Id.* § 5. S. 773 does not reach depositary institutions or providers of securities and insurance products. Jurisdiction over depositary institutions is with the Senate Committee on Banking, Housing, and Urban Affairs. Committee Information, U.S. SENATE COMMITTEE ON BANKING, HOUSING & URBAN AFFAIRS, http://banking.senate.gov/public/index.cfm?FuseAction=CommitteeInformation.Jurisdiction (last visited Aug. 27, 2010).

189. S. 773 § 6(a).

190. *Id.* § 14(a).

191. *Id.* §§ 6, 14. The breadth of this authority would allow the Secretary of Commerce to avoid the requirements of the Federal Right to Financial Privacy Act, 18 U.S.C. §§ 3401–3422 (2006), and of other federal pro-privacy protections in the Fair Credit Reporting Act, 15 U.S.C. § 1681(u)–(v) (2006), the Electronic Communications Privacy Act, 18 U.S.C. § 2701(a) (2006), and the National Security Act, 50 U.S.C. § 401 (2006). In the absence of restrictions such as these, the government could obtain any information that an individual voluntarily gave to a third-party or that resulted from their transactions.

192. *See* S.773—Cybersecurity Act of 2009, OPENCONGRESS, http://www.opencongress.org/bill/111-s773/show (last visited Aug. 29, 2010) (citing S. 773 § 18(2)); *see also* James Corbett, *The Rising Tide of Internet Censorship,* GLOBAL RESEARCH (Feb. 5, 2010), http://www.globalresearch.ca/index.php?context=va&aid=17433 (reporting, among other things, the finding in conjunction with the bill's introduction in 2009 that "'voluntary action is not enough'" to manage cyber security threats) (citation omitted).

d. S. 3027—The P2P Cyber Protection and Informed User Act

S. 3027, the P2P Cyber Protection and Informed User Act, is a companion bill to H.R. 1319, which was introduced on February 23, 2010.[193] Its substance is identical to that of H.R. 1319, described in Section IV.A.1.a of this Article, *supra*.[194]

B. STATE LEGISLATION

While the federal government has been trying to enact and consider data security bills, at least forty-six states, and the District of Columbia, Commonwealth of Puerto Rico, and the U.S. Virgin Islands have enacted some form of data security breach notification requirements.[195] One state has enacted a provision that requires retailers whose conduct causes payments data spills to compensate the parties with whom they have dealt,[196] and a second is considering imposing a statutory contributory negligence standard[197] as well as a fund to which merchants would contribute on a per-transaction basis to manage compensation for victims of payments data security breaches.[198]

1. General Observations on State Data Security Breach Laws

State law requirements that make vendors liable to financial institutions for breaches of unencrypted credit and debit card payment transaction data could make a big difference in the overall integrity of the payments system. To date, only Minnesota has enacted legislation that creates incentives to deter breaches in this manner.[199] The Minnesota law requires the use of PCI,[200] the only state to do so. It also imposes liability on merchants for data security breaches.[201] The forty-five other states that have required breach notices to affected consumers create incentives for stronger

193. P2P Cyber Protection and Informed User Act, S. 3027, 111th Cong. (as introduced, Feb. 23, 2010).

194. *Id.*; *see supra* Part IV.A.1.a.

195. State Security Breach Notification Laws, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=13489 (last modified Apr. 12, 2010). For an excellent discussion of the variables in state data security laws, see G. Martin Bingisser, Note, *Data Privacy and Breach Reporting: Compliance with Various State Laws,* 4 SHIDLER J.L. COM. & TECH. 9 (2008), *available at* http://www.lctjournal.washington.edu/Vol4/a09Bingisser.html (written when about half the states had enacted data security breach notification laws).

196. MINN. STAT. § 325E.64 Subd. 6 (2009); MINN. STAT. § 8.31 Subd. 3 (2009).

197. 2010 H.B. 1149, 2010 Leg., 61st Sess. (Wash. 2010).

198. An earlier version of Wash. 2010 H.B. 1149 contained the authority to collect the two-cent fee to establish the fund. *Data Security: Amended Bill Assigning Payment Card Breach Liability Passes Washington House,* Banking Rep. (BNA) No. 94, at 429 (Mar. 2, 2010) [hereinafter *Amended Bill Passes WA House*].

199. § 325E.64; *see also* James T. Graves, Note, *Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care*, 34 WM. MITCHELL L. REV. 1115, 1117, 1132 (2008).

200. § 325E.64.

201. *Id.* Subd. 3.

technical, administrative, and physical safeguards for payments data by requiring notice to all consumers whose personally identifiable information has been released in a security breach.[202]

But each state's laws vary slightly, and many employ subjective or objective thresholds before action is required. For example, Washington's statute relieves an individual or entity from the duty to disclose the breach if the breach "does not *seem* reasonably likely to subject customers to a risk of criminal activity."[203] Virginia's standard is both objective and similarly subjective; disclosure of the breach is required if:

> [I]nformation is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity [suffering the breach] reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.[204]

Reliance on the subjective assessments of the entity suffering the breach may be likely to produce too little notification and, therefore, too little customer or public pressure to reform data security practices.

State data security breach laws often do not provide much in the way of direct redress for consumers whose payments transaction data is compromised. For example, the Indiana security breach statute does not create a private right of action for consumers.[205]

Other state proposals use high thresholds, such as the restriction in H.B. 1149 in Washington limiting its application to businesses and government agencies that process 6 million or more payment card transactions in a year,[206] and also (perhaps incorrectly) exempts businesses or agencies from liability provisions if they are in compliance with PCI DSS[207] (because compliance ends when a breach is demonstrated). The varied requirements of these state laws undoubtedly have contributed to the numbers of data security bills introduced in Congress, as interstate companies work to preempt with inconsistencies across states. [208]

State breach notification statutes may be seen by some as comparable to the outbreaks of "domestic legislation" that from time to time propelled

---

202. *See, e.g.*, *id.* Subd. 3(5).

203. WASH. REV. CODE ANN. § 19.255.010(d) (West 2010) (emphasis added).

204. VA. CODE ANN. § 18.2-186.6(C) (West 2010).

205. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 637 (7th Cir. 2007) (adding that the Indiana statute "imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow").

206. *See Amended Bill Passes WA House*, *supra* note 198.

207. *Id.*

208. Thomas M. Lenard & Paul H. Rubin, *Much Ado About Notification: Does the Rush to Pass State-Level Data Security Regulations Benefit Consumers?*, REGULATION, Spring 2006, at 44, 49–50, *available at* http://www.cato.org/pubs/regulation/regv29n1/v29n1-5.pdf.

amendments to MARPOL's requirements.[209] The varying compliance responsibilities of separate state laws and their costs likely draw funds[210] and energy away from technical innovations aimed at overall safety goals. In the data security context, however, the willingness of states to enact data security breach laws has had the benefit of "increase[ing] the visibility" of data security.[211]

C. NOVEL STATE PROPOSALS TO REDRESS OR DETER PAYMENTS DATA SECURITY BREACHES

H.B. 1149, the bill that the Washington legislature passed,[212] originally suggested two new means of redressing liability. First, it made vendors that sell payment card processing software and equipment contributorily liable for breaches caused by faults in their software or hardware.[213] Also, it allowed merchants to charge two cents per transaction to offset the costs of the insurance merchants would have to cover their liability to financial institutions should data that merchants retained be breached.[214] Only the former of these made it though Washington's House of Representatives.[215] The bill also prohibits merchants "from retaining credit card security code data, PIN codes or verification numbers, or the full content of 'magnetic stripe data' after authorization of a transaction without the express consent of customers."[216] In addition, it makes retailers liable for breaches of retained payment card data if the breach affected 5,000 or more unencrypted individuals' names or account numbers, as long as the business or agency processes 6 million or more payment card transactions per year.[217] This provision is unique in that it limits *liability* to cases in which the breach reaches a threshold number, as opposed to the more standard numerical trigger for *notices of the breach to consumers*. If this provision is

---

209. *See, e.g.*, Maitland*, supra* note 102, at 52; *Senator Lautenberg—Naval Architect?,* MARINE LOG, Apr. 2008, at 14 (describing the October 2006 amendments to MARPOL and the notion that if the International Maritime Organization moves in "too 'reasonable' [a manner] it may not fend off unilateral action by individual countries").

210. Caroline Stenman, The Development of the MARPOL and EU Regulations to Phase Out Single Hulled Oil Tankers 8, 23–24 (May 2005) (masters thesis, Goteborg University School of Economics and Commercial Law), *available at* http://gupea.ub.gu.se/bitstream/2077/1941/1/2005 56.pdf (explaining how unilateral EU action spurred adoption of stricter MARPOL guidelines, phasing out single-hulled ships more quickly); *see generally* Michael E. Porter & Claas van der Linde, *Toward a New Conception of the Environment-Competitiveness Relationship,* 9 J. OF ECON PERSP. 97, 113–14 (1995); Roy Rothwell, *Industrial Innovation and Government Environmental Regulation: Some Lessons From the Past,* 12 TECHNOVATION 447 (1992).

211. Graves, *supra* note 199, at 1116.

212. 2010 H.B. 1149, 2010 Leg., 61st Sess. (Wash. 2010), *amending* WASH REV. CODE § 19.225.RCW (2010).

213. *Id.* § 3(b).

214. *Amended Bill Passes WA House*, *supra* note 198.

215. *Id.*

216. *Id.*

217. *Id.*

enacted, it could establish a precedent of non-liability for breaches affecting only smaller numbers of individuals, which would not create incentives for stronger data security.

V. ARE "SAFE HARBORS" OR PRESUMPTIONS BASED ON ENCRYPTION OR OTHER SECURITY METHODS APPROPRIATE?

As mentioned above, some of the data security bills pending in Congress provide exemptions from requirements *to notify individuals* whose personally identifiable information may have been affected by the data security breach if the holder of the information has had the data encrypted or subject to some other security methods. In some cases, exemptions are possible based on *encryption alone*. This approach is used in Ohio, West Virginia, and Virginia.[218] In other cases, use of encryption alone is sufficient to establish a *presumption that there is no significant risk that personally identifiable information was exposed in the breach.*[219] Encryption alone does not prevent attacks: data in the Heartland breach was encrypted at the store, but apparently not in transmission.[220]

In early 2010, at a lecture on encryption given by Indiana University School for Informatics Professor Steven A. Myers,[221] I asked a question about basing a "safe harbor" for data security on encryption alone. The reaction by the Informatics faculty and graduate students in the room was immediate and visceral: *their jaws dropped.* Their ensuing remarks made it clear their collective belief that encryption alone should not suffice to qualify for a safe harbor. Rather, they preferred a combination of encryption

---

218. Many states create safe harbors by defining personal information as unencrypted and readable data elements. *See, e.g.*, OHIO REV. CODE ANN. § 1347.12(A)(6)(a) (West 2010). Other states create safe harbors by defining a breach as "unauthorized access and acquisition of unencrypted and unredacted data." W. VA. CODE ANN. § 46A-2A-101(1) (2010). Others create explicit safe harbors. *See, e.g.*, VA. CODE ANN. § 18.2-186.6(C) (West 2010).

> An individual or entity shall disclose the breach . . . if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.

VA. CODE ANN. § 18.2-186.6(C).

219. Several states define "significant risk" as excluding the breach of encrypted data. *See, e.g.*, R.I. GEN. LAWS § 11-49.2-3(a) (2010) ("Any state agency or person . . . shall disclose any breach of the security of the system which poses a significant risk of identity theft . . . to any resident of Rhode Island whose unencrypted personal information was [breached] . . . .").

220. *See Heartland Hacker Gonzalez Pleads Guilty to Compromise of Over 170 Million Cards,* ATMMARKETPLACE.COM (Sept. 14, 2009), http://atmmarketplace.com/article.php?id=11319&na=1 [hereinafter *Heartland Hacker Pleads Guilty*].

221. Steven A. Myers, Lecture at the Maurer School of Law, Indiana University: One Bit Encryption (February 16, 2010). For the text of the paper on which this lecture was based, see Steven Myers & Abhi Shelat, Bit Encryption Is Complete (2009) (unpublished manuscript) (on file with author).

and "best practices" involving administrative, technical, and physical safeguards. Dr. Meyers and others in that audience also noted that the value of encryption also depends to some extent on the portions of the data and data transmission to which encryption is applied and the manner through which the data were obtained. For example, the group of thieves responsible for the TJX and Hannaford Brothers data spills were engaged in diverse strategies including one known as "war driving" in which the group intercepted payments data during transmission over wireless Internet connections by positioning themselves close to store locations from which the data were being transmitted.[222]

VI. ARE RECENT PAYMENTS DATA SECURITY DEVELOPMENTS MOVING CLOSER TO A MARPOL-LIKE REGIME?

Data security laws in the United States normally do not mandate that a particular form of data security/anti-fraud process be employed, with Minnesota's law as the possible vanguard of a new approach.[223] Rather, existing state laws impose requirements on the owner of data if a data security breach occurs.[224] Thus, the norm is to allow the marketplace to devise means to protect data so as to avoid the expense and reputational risk of revealing that a data security breach occurred. This places the responsibility of protecting data on each entity that holds payments data and related personally identifiable information. One advantage of this approach is that there is no single standard method of protecting payments data; the diversity of approaches serves as a barrier to easier hacking, and there is no static standard that would require legislative action to amend. However, as reports of the "iffy decisions" made by BP and its partners in the drilling of the Deepwater Horizon well show,[225] self-driven risk assessments in highly competitive environments may result in the commitment of too few resources to disaster prevention.[226]

Payments systems and others could create more incentives for users to keep up-to-date in deploying new security. They could, for instance, require software developers to warrant their programs (as discussed in subsection A below) or could push towards adoption of more secure technologies (as discussed in subsection B).

---

222. Indictment at 4–5, United States v. Albert Gonzalez, No. SBK/EL/2009R00080 (D. N.J. 2009). Gonzalez has since pled guilty to identity theft, wire fraud, computer fraud, and conspiracy in Massachusetts and New York, though charges are still pending in New Jersey. *See Heartland Hacker Pleads Guilty, supra* note 220.

223. Graves, *supra* note 199, at 1117.

224. State laws typically impose duties to disclose and/or compensate after a breach has occurred. *See, e.g.*, CAL. CIV. CODE §§ 1785.11.2, 1798.29(a) (West 2007).

225. *See* Achenbach & Hilzenrath, *supra* note 39.

226. *See* Stephens, *supra* note 3.

A. SECURITY BASED ON SOFTWARE & WARRANTIES

Beyond requirements for prevention of payments data spills that are comparable to MARPOL's, some commentators have suggested that we should use different methods to make payments systems software less susceptible to hacking, including for example by requiring providers of software and database operators to warrant their products or their services to end users. Two of the proponents of specialty payments data warranties are Roland Trope[227] and Professor Juliet Moringiello.[228]

Warranties are a common way to manage externalities and to overcome asymmetries in information between manufacturers and providers of services and their customers.[229] Warranties in sales transactions include express and implied warranties of merchantability and fitness for a particular purpose, as well as warranties of good title and quiet enjoyment, and warranties against infringements of patents and trademarks.[230] In the payments data security arena—as in other vertical manufacturing and retailing environments—warranties present some attractive market opportunities for providing remedies if software fail to deliver their promised results or services do not protect data in transmission or storage.

In 2004, Roland Trope argued for the creation of a software "limited cyberworthiness warranty" based on the doctrine of seaworthiness.[231] He made two observations that bear upon both the focus of this Article and his cyber-worthiness proposal. First, he explained that common law in the United States treats ships as "unseaworthy when [they are] 'insufficiently or defectively equipped.'"[232] He also observed that "[c]ourts have come to regard the seaworthiness of a ship as analogous to a warranty."[233]

As Mr. Trope conceives of this new limited warranty, its target is the capacity of a software "application's capabilities to protect confidential information from unauthorized access from, or disclosure to, cyberspace."[234] He proposes that such a warranty might require that:

---

227. Roland L. Trope, *A Warranty of Cyberworthiness,* IEEE SECURITY & PRIVACY, Mar./Apr. 2004, at 73 [hereinafter *Cyberworthiness*].

228. *See generally* Moringiello, *supra* note 12.

229. *See* Claire A. Hill, *A Comment on Language and Norms in Complex Business Contracting*, 77 CHI.-KENT. L. REV. 29, 42 (2001).

> Contractual provisions, typically representations and warranties, serve to credibly communicate information, chiefly to rebut the presumption of undesirable attributes which divergent interests inspire and information asymmetry makes possible. They provide a means for one party to signal to the other the absence of undesirable attributes and presence of desirable attributes.

Id.

230. U.C.C. §§ 2-312–315 (2003).

231. *Cyberworthiness, supra* note 227, at 73–74.

232. *Id.* at 74 (citing Waldron v. Moore-McCormack Lines, Inc., 386 U.S. 724, 726 (1967)).

233. *Id.* at 74 (citing Brister v. A.W.I., Inc., 946 F.2d 350, 355 (5th Cir. 1991)).

234. *Id.* at 73.

- Prior to the software's release, the maker subjected [the software] to rigorous tests to verify its degree of security against intrusion by unauthorized persons, electronic agents, or code (that is, it verified its cyberworthiness).
- By the time of release, the maker [should have] removed all known critical security vulnerabilities found in the software. (I define "critical" as any vulnerability that, if exploited, would enable unauthorized access to confidential information or unauthorized control of a user's computing device.)
- After release, the maker shall continue to diligently probe the software for security vulnerabilities.
- When the maker learns of a critical vulnerability, it will immediately email all high-priority customers, describe the problem in detail, and provide suggestions for a temporary solution—disabling features, and so on—to diminish or limit the vulnerability until the maker can provide a patch. ("High-priority customers" are those likely to have valuable confidential information at risk in systems linked to cyberspace. To become such a customer, the party would enter into a written agreement with the software maker that any vulnerabilities disclosed and patches released to it would be kept confidential to prevent hackers from gaining early knowledge of such vulnerabilities. These customers would pay an increased purchase price in exchange for the incremental increase in protection.) The vulnerability notice also would include information that would alert users to take additional precautions to safeguard their confidential information until they had received a security patch.
- Immediately after creating a vulnerability security patch, the maker would email it first to the high-priority customers and, after an interval, to all registered software users.
- When distributing a security patch, the software maker shall not attach to it any disclaimer as to the accuracy of information provided with the patch or its fitness for correcting the specified security vulnerability. . . .
- The software's warranty will be valid for a period of three years from the release date. (A security patch or newly marketed software should be warranted for a period comparable to that covered by the computing device's warranty. It should be a period long enough to earn a user's trust. . . .
- The warranty would be valid for purchasers who buy directly from the maker and for those who buy from third-party sellers, but [whose purchaser is] still in the direct chain of distribution from the maker.

- The warranty would prescribe precautions to which purchasers must adhere, such as "do not open unknown attached files in emails from unknown senders." Purchasers who violate the precautions (and suffer or cause harm) void the warranty, and will not be entitled to damages from the maker.
- If the maker breaches the warranty, the purchaser (buyer or licensee) is entitled to an expeditious remedy of a liquidated damage in an amount and through a procedure specified in the warranty . . . .[235]

Mr. Trope also proposes that this cyber-warranty be "phased in . . . with the first security-patch release."[236] In addition, he suggests that warrantors "would offer only the portion of the proposed warranty that applies to each patch."[237]

Professor Moringiello urges a warranty like the homeowners' warranty (HOW) that first became popular in the late 1970's.[238] She analogizes to early warranties created by law in which courts were unwilling to allow injured end users no remedy as against a provider with superior knowledge and the ability to control the end product through contract and preventive measures.[239] Although courts have been far more reluctant to create warranties in the data security arena, the theories undergirding early common law warranties and the original common law homeowners' warranties[240] may apply with equal force to payments data security.

To allay payments-related data security concerns, the United States and others will need to employ both MARPOL-based approaches and warranties such as Trope's phased-in cyber-worthiness warranty and Moringiello's HOW-like proposals. PCI DSS—a certification process based on technical standards[241]—represents a significant advantage in protecting the whole electronic payments data chain, but problems nevertheless have arisen within systems that recently had been judged PCI DSS compliant. For example, Hannaford Brothers apparently met credit card industry security standards prior to breach but was still vulnerable to hacking.[242]

---

235. *Id.* at 73–74.
236. *Id.* at 74.
237. *Id.*
238. Moringiello, *supra* note 12, at 80–82.
239. *Id.*
240. *See id.*
241. For a description of the PCI DSS standards as well as the opportunity to download them, see PCI SSC Data Security Standards Overview, PCI SECURITY COUNCIL, https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (last visited Dec. 30, 2010).
242. *See* Ross Kerber, *Advanced Tactic Targeted Grocer 'Malware' Stole Hannaford Data*, BOS. GLOBE, Mar. 28, 2008, at 1A (noting that Hannaford met standards set by VISA, Inc. and other card companies but that these were not sufficient to avoid the breach, explaining that the breach was attributable to that which analyst Steve Rowen described as "'markedly more

B. SECURITY BASED ON THE CARDS THEMSELVES OR ON THE CARD AND THE CARD AUTHENTICATION PROCESS:

More recent payments security advances include "chip-and-PIN" systems associated with the Europay, MasterCard, and VISA (EMV) system. EMV generates transaction data from the "card authentication [process] and from the cardholder verification processes" the issuer may employ.[243] Deployed in the EU, Canada, and Asia beginning in 2004, and mandatory in the UK beginning in 2005, chip-and-PIN technologies offer more protections against hacking.[244] For example, in the first year of its deployment in the UK, chip-and-PIN technology contributed to a 13 percent decline in card fraud in Britain.[245] However, as a "skimming" fraud[246] aimed at Shell oil stations in the UK in 2006 demonstrated, for cards that contain magnetic stripes as well as EMV/chip-and-PIN technology, even EMV is not fail-safe.[247] And, as Jane Adams reports, thieves can still perpetrate "card-not-present" frauds by bypassing the chip or magnetic stripe.[248]

Despite the issues with these technologies, EMV/chip-and-PIN technologies offer more advanced anti-fraud approaches, including the ability to "identify fraud patterns and credit risk situations" by comparing data gleaned from the current transaction to data from prior transactions.[249] However, EMV technology has been slower to gain traction in the United

---

sophisticated,'" and reporting that the hackers "mined a stream of data that merchants and banks were not responsible for protecting under industry rules").

243. Jane Adams, *Dynamic Risk Management with EMV Data*, ACI WORLDWIDE, July 2006, at 1, http://surveycenter.tsainc.com/pdfs/3065%20EMV%20flyer.pdf (citing Michael Hendry, a payments consultant who helped implement EMV systems in the EU).

244. *See, e.g.*, *Fed Official Warns Card Fraud Threat Growing in U.S.*, COLLECTIONS & CREDIT RISK (July 27, 2010), http://www.collectionscreditrisk.com/news/fed-official-warns-card-fraud-threat-growing-3002682-1.html (citing Richard Oliver of the Atlanta Federal Reserve Bank's Retail Payments Risk forum advocating for shift to EMV smart-card technology to thwart fraud rings and criminals used in Europe, Canada, and other regions of the world); Fitzgerald, *supra* note 41 (describing phase-in deadlines for EMV technology in Canada and liability increases for merchants that have not deployed it on schedule); Brian Ooi, *The EMV Migration Path in the Asia Pacific Region*, FROST & SULLIVAN (Aug. 25, 2005), http://www.frost.com/prod/servlet/market-insight-top.pag?docid=46281303; Vijayan, *supra* note 80.

245. Adams, *supra* note 243, at 1.

246. *See Petrol Station Worker Admits Credit Card Fraud*, NORTHAMPTON CHRON. & ECHO (U.K.), Apr. 9, 2009, http://www.northamptonchron.co.uk/news/Petrol-station-worker-admits-credit.5156481.jp.

247. Adams, *supra* note 243, at 1.

248. *Id.*

249. *Id.* at 2. Adams reported that information stored on the card and capable of being passed back through EMV includes information relevant to prior efforts to misappropriate the card and the authorization process such as evidence that data authentication, script processing, or authorization request cryptogram verification has failed. *Id.* Card data also would show repeated uses at untended terminals. *Id.* Some of the data that the card can send pertain to offline transactions, which Adams reported are "particularly prone to fraud." *Id.*

States[250] than in Europe[251] and the absence of EMV chips is an obstacle to U.S.-based consumers using their cards for international travel.[252] Among the issues that may work against broader-scale deployment in the U.S. are the costs of the readers[253] for EMV cards and concerns that full-deployment of the cards featured could implicate privacy concerns.[254]

CONCLUSION

The cost and extent of payments-related data security breaches have been rising in the United States.[255] Legislation to curb data security breaches and to enhance enforcement of federal laws that have emanated recently from the Committee on the Judiciary in the House of Representatives and the Senate Committees on the Judiciary, Homeland Security, and Commerce, Science and Technology offer promise. These bills are steps in the right direction but they still suffer from the jurisdictional limitations under which the Senate Committees in particular

---

250. *See Chips Cards in the U.S.,* THE NILSON REPORT ISSUE 930, at 6 (July 2009) (explaining most U.S. issuers will have EMV-compliant chip cards available by the end of 2010 with plans to market them to upscale frequent international travelers). The slow adoption of chip-and-PIN technology has made it harder for individuals with credit cards issued in the U.S. to use them abroad. *See* Michelle Higgins, *For Americans, Plastic Buys Less,* N.Y. TIMES, Oct. 4, 2009, at TR3 (explaining that 22 countries including "much of Europe, Mexico, Brazil, and Japan, have adopted the technology" and that another 50 countries are "in various stages of migrating to the technology in the next two years, including China, India, and most of Latin America"). In addition, Ms. Higgins reported that as Canada deploys this technology issuers there "plan[] to stop accepting magnetic stripe debit cards at A.T.M.s after 2012 and at point-of-sale terminals after 2015." *Id.* For more information on Canada's movement to chip-and-PIN technology, see *Canada's Migration to Chip,* EMV CANADA, http://www.emvcanada.com/merchant_documents/background.pdf (last visited Dec. 30, 2010). EMVCanada is a web site provided by ACT Canada, a non-profit organization, to provide a neutral forum for consumers, merchants, and the media to learn and share information related to secure payments. *Id.*

251. *See* Brandon Glenn, *Visa Hopes European Unit Can Give More Flexibility to Customers,* IRISH TIMES, May 7, 2004, at 58 (discussing the introduction of chip-and-PIN systems throughout Europe).

252. *EMV Chip Cards Expected for Upscale U.S. Cardholders,* SMART CARD ALLIANCE, http://www.smartcardalliance.org/resources/pdf/EMV_Cards_Issued_in_US.pdf (last visited Sept. 22, 2010).

253. *See* Dan Balaban, *Turning the Corner,* CARD TECH., Nov. 1, 2005, at 42 (reporting on the slow roll-out of readers across Europe).

254. Adams*, supra* note 243, at 2–3 (discussing the capacity to build a "detailed user profile"). Chipped cards are capable of holding significant amounts of personal data, such as passport and driver's license information, health records, and medical histories. *See Fundamentals of EMV Chip: The Next Revolution: The Payment Environment Is Quickly Changing. Are You Ready to Make Contact in this Brave New World?,* INSIGHTS, Winter 2006, at 4, *available at* http://www.mastercard.com/ca/wce/PDF/14049_Insights2006-Fundamentals-EN.pdf [hereinafter *Fundamentals of EMV Chip*].

255. *See* PONEMON INSTITUTE, *supra* note 23, at 4. For a more comprehensive discussion of card payment fraud, particularly its potential for damage and increases in fraud, see Richard J. Sullivan, *The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options,* FED. RESERVE BANK OF KANSAS CITY ECON. REV., 2Q 2010*,* at 101.

operate.[256] These jurisdictional limitations caused the current gaps in data security left by GLBA,[257] FACTA,[258] and HIPAA.[259] Thus, the more recent bills described in this paper—apart from S. 773—focus on "data brokers," commercial entities whose primary role is to collect and sell post-transaction information including personally identifiable information, as opposed to persons who themselves engaged in transactions with consumers whose personal and account information is the target of thieves or those already are governed as "consumer reporting agencies" by the Fair Credit Reporting Act and FACTA.[260]

These bills will impose on data brokers particular federal requirements, but will leave them unconnected legally to end users, that is, the consumers or businesses whose transaction information they have obtained will still be without legal recourse against the entity that was holding their data at the time of the breach.[261] For this reason, the lack of a unified regulatory regime operating on an end-to-end basis leaves the door open to future database hacking because of decisions such as that by the Supreme Judicial Court of Massachusetts in *Cumis Insurance Society, Inc. v. BJ's Wholesale Club, Inc.*[262] Moreover, Congressional bills, such as H.R. 2221 and S. 1490, which grant a safe harbor from prosecution for violations of their requirements, including the requirement to notify affected individuals if the data are encrypted or the entity uses other "best practices" to bolster the benefits of encryption, are likely to leave a lot of account data and other personally identifiable information without sufficient protection.[263]

---

256. For example, it apparently is much more difficult in the Senate to take up a subject or to propose a law governing an industry that lies partly in the jurisdiction of another committee. Thus, each committee drafts legislation uniquely aimed at solutions to issues within its own purview, often leaving associated issues unresolved for jurisdictional reasons. Senate Committees, U.S. SENATE, http://www.senate.gov/artandhistory/history/common/briefing/Committees.htm (last visited Oct. 2, 2010).

257. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

258. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952.

259. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 16, 26, 29, 42 U.S.C.).

260. Fair Credit Reporting Act, 15 U.S.C. § 1681a(f) (2006).

> The term 'consumer reporting agency' means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

Id.

261. *See supra* text accompanying notes 149–194.

262. Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc. 918 N.E.2d 36, 46–47, 50–51 (Mass. 2009).

263. *See* Data Accountability and Trust Act, H.R. 2221, 111th Cong. § 3 (as passed by House, Dec. 8, 2009); Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. § 311 (as reported by S. Comm., Nov. 5, 2009).

The current enacted and proposed legislation addresses many of the similarities between data spills and maritime accidents. But, unfortunately, many of our data security efforts to date seem to miss the most critical distinction between legal schemes for the prevention of pollution from maritime accidents and other legal prevention schemes: that payments-related data security breaches are different from the hazards of maritime activities. It is important to remember Roland Trope's highly useful observation that it is easier for ships to avoid encounters with charted rocks and shallow waters than with shifting sand bars.[264] The former do not move. Sand bars move, and their movement may be accelerated by storms and other weather conditions. But even sand bars are better known risks than data-security attacks. Sand bars and other natural maritime risks move much less frequently and normally with more predictability than does the capacity, indeed the determination and artistry, of individuals determined to penetrate databases or to intercept real-time exchanges of payments-related data.

Maritime accidents fall into two categories—collisions between two ships, or accidents involving the oil-and-gas exploration or the operation of deepwater ports, which are primarily the result of operator negligence, on the one hand, and groundings or collisions with rocks, sand bars and shoals, and other inherent sea hazards.[265] Payments data security breaches seem more closely associated with the former category because cost-cutting and inadequate risk assessments by private actors contribute to disasters with broad-reaching implications, as the Deepwater Horizon explosion and spill tragically demonstrated.[266] But payments-related data spills are even harder to prevent because, unlike events caused by storms, negligence, or merely bad choices, data security breaches are perpetrated by determined individuals who are constantly exploring new methods of getting access to data and systems they need to engage in crimes. Thus, in payments-data security, the "terrain"-based threats seem to be subject to even more constant changes than are sand bar risks to maritime activities.

Like MARPOL and the associated compensation conventions—such as Civil Liability 1992 and Fund 1992, and their predecessors[267]—we should make data protection a dynamic process that receives persistent attention, specifically by rethinking and restructuring it as new means of safeguarding against data protection penetration as administrative, technical, and physical safeguards come into being. Encryption is one of the technical safeguards

---

264. Interview with Roland Trope, *supra* note 147.

265. *See supra* text accompanying notes 139–146; *see also* Graham Mapplebeck, Int'l Mar. Org., Navigational Safety and the Challenges of Electronic Navigation (Feb. 14, 2008) (transcript available at https://www.imo.org/includes/blastDataOnly.asp/data_id%3D21091/Navigationalsafety.pdf).

266. *See* Achenbach & Hilzenrath, *supra* note 39.

267. *See supra* text accompanying notes 98–133.

that should be part of this process, but it alone is insufficient to protect data, counter-parties, or consumers.

Moreover, despite traditional and appropriate reluctance in this country to require that certain technologies be employed, developments elsewhere may make the use of specific technologies, comparable to the double-hull requirement in MARPOL,[268] mandatory. For example, with EMV increasingly in use in the EU and Canada, it may only be a matter of time before EMV is more widely used here by credit and debit card issuers. However, while EMV technologies can contribute to greater fraud prevention, they do not yield 100% protection from fraud[269]—and their protection may come at the price of consumer/user privacy.[270]

Third, despite the widespread damage that a maritime accident may create, the causes and effects of data spills are much less localized than the effects of typical maritime accidents. Data security breaches of a system in one part of the world—such as the penetration of Royal Bank of Scotland's WorldPay system and the rapid subsequent withdrawals at ATMs in forty-nine countries[271]—affect payments systems in other parts of the world.[272]

Fourth, Congress and the states have crafted legislation that addresses consumer concerns more than actual prevention of payments data spills. With the exception of S. 773, the other bills discussed in this Article require consumer notification once the spill has occurred if the owners' assessments of the number of consumers affected exceed specified thresholds and also address certain limited law enforcement concerns.[273] But they generally leave risk-assessment and choices of administrative, technical, and physical safeguards for systems and data to the private actors involved.

Consumers in a breach-prone environment are a lot like birds, fish, and other animals whose habitats are affected by spills of hazardous substances they did not cause. They often lack the ability to protect themselves. However, in the data security environment, consumers with access to information concerning data spill events may be better able to thwart additional damages to their financial well-being such as identity theft and credit-rating damage. However, at this time in the United States, as

---

268. Revised Annex 1 of MARPOL 73/78, *supra* note 105.

269. Adams, *supra* note 243, at 1.

270. *Fundamentals of EMV Chip*, supra note 254, at 4.

271. *See* Part I.A.1; *see also* Ashford, *supra* note 70; Espiner, *supra* note 65; Lemos, *supra* note 66.

272. Lemos, *supra* note 66 (persons acting in concert with the hackers were located in forty-nine cities around the world and accessed roughly 130 ATM's in their respective areas to carry out the last phase of this payments fraud). In the longer-standing attack announced by the FTC in February, the perpetrators used multiple command and control centers around the world to manage their money movements. Robert McMillan, *SEC, FTC Investigating Heartland After Data Theft*, PCWORLD (Feb. 25, 2009, 6:10 PM), http://www.pcworld.com/businesscenter/article/160264/sec_ftc_investigating_heartland_after_data_theft.html.

273. *See supra* text accompanying notes 163–198.

described in this Article, there is no standard requirement for disclosure, and in some states disclosure is limited to large-scale data spills, such as the 6-million-payments-card processed-per-year threshold in Washington State's H. 1149.[274] Even consumers who might consider switching to new providers or to other retailers after a data-spill event affected their former provider or favorite grocery chain, there are few guarantees that the security systems that their new providers employ are any less vulnerable to a breach than their former providers' systems were.

Similarly, some data spills cause other providers' systems to become infected, in a manner like Deep Water Horizon or the Exxon Valdez in which oil spread away from the primary location.[275] Accordingly, entities that own or possess payments data should receive legal or other financial incentives to employ ever-strengthening administrative, technical, and physical protections for data related to consumer deposit accounts, credit cards, debit cards, and other prepaid cards, as well as for other types of financial accounts such as insurance and securities. And there should be adequate legal consequences of failing these duties to maintain adequate safeguards beyond those already codified such as the rules implementing GLBA, FACTA, and other federal statutes and rules, including appropriate private rights of action provided by relevant federal statutes or fines as the OPA allows.[276]

As EMV/chip-and-PIN technologies deploy around us,[277] they probably will become the standards for retail payments security. EMV and PCI DSS are different solutions to these issues, employed in different nations, to protect the integrity of card-based payments. EMV and PCI DSS represent different philosophies for providing protection on the order of MARPOL's double-hulled ship scheme. However, employing some security technology such as EMV imposes a real trade off in the form of privacy, because the technology can retain more information about purchasing habits than other card systems retain on the card itself.[278] This does not present the same types of concerns in Canada or the EU as it may in the U.S. because of the restrictions on trading the types of information that EMV technologies and other payment card transactional records may contain. This concern would grow larger if legislation such as S. 773 is enacted because it grants open-ended access to information to the Secretary of Commerce, without mention of any restrictions on retention or other use of the information unconnected with prosecution and resolution of the data security breach.[279] Thus, it could

274. 2010 H.B. 1149, 2010 Leg., 61st Sess. (Wash. 2010), *amending* WASH REV. CODE § 19.225.RCW (2010).

275. *See supra* Part III.

276. *See supra* text accompanying notes 42–55.

277. Deployments in Canada and Mexico are considerably ahead of deployment in the U.S. *See EMV Chip Cards Expected for Upscale U.S. Cardholders*, *supra* note 252, at 1 n. 5.

278. *Fundamentals of EMV Chip*, *supra* note 254.

279. *See* Cybersecurity Act of 2009, S. 773, 111th Cong. § 14(b) (2009).

enable a vast warehousing of payments transaction data by Commerce without protections already applicable to other government data requests or collection.[280]

Among the solutions discussed in this Article, the types of cyber warranties that Mr. Trope and Professor Moringiello have advocated are attractive so long as they cannot be disclaimed, depriving end users and consumers of their protections. New data security warranties could be enacted at the state level, or by Congress, or could form part of a MARPOL-like multilateral approach with its prescriptive regulation of aspects of accident prevention and intentional shipping discharges of oil and other pollutants—such as its double-hull and operational requirements, as well as its additional operational requirements or "penalties" on ships that do not comply.[281] MARPOL's requirement of notice of spills and discharges to a central agency is similar to proposals in Congress that require notice to the U.S. Secret Service.[282] Notice allows a government authority to monitor recovery processes and to coordinate law enforcement resources as needed.

However, in terms of compensation for victims of shipping spills and discharges and oil-and-gas exploration accidents, neither MARPOL nor the Oil Liability provisions of the Clean Water Act offers optimal solutions for the payments data security breach arena for at least two reasons. First, unlike shipping or exploration events that are unlikely to repeat themselves, payments data breaches may recur or thieves may use and/or resell the information they obtain. Second, once liability limits are enacted in statutes or agreed to in treaties or conventions, they are difficult to raise.[283]

Enabling stronger deterrence of, and finding means of resolving payments data security breaches when they occur, is vitally important to the integrity of the payments system and to individuals' trust of it. We should strive for more seamless recovery methods than are currently available in

---

280. *Id.* ("The Secretary of Commerce—(1) shall have access to all relevant data . . . without regard to any provision of law, regulation, rule, or policy restricting such access.").

281. Revised Annex I of MARPOL 73/78, *supra* note 105.

282. Data Privacy and Security Act of 2009, S. 1490, 111th Cong. § 316 (as reported by S. Comm., Nov. 5, 2009); *see also* S. REP. NO. 111-110, at 5 (2009) ("[T]he bill also requires that business entities and Federal agencies notify the Secret Service of a data security breach within 14 days of the occurrence of the breach.").

283. *E.g.*, Mailtland*, supra* note 102, at 51. As an example of how long a ceiling or floor stays in a federal statute, consider the Truth in Lending Act, 15 U.S.C. §§ 1601–1693r (2006). Since its original enactment in 1968, it has exempted transactions in which the total amount financed exceeds $25,000. *Id.* § 1603(3); *see also id.* § 1601. Certainly, $25,000 bought a lot more in 1968 than it would today. In the oil spill context, Senator Lautenberg of New Jersey has introduced legislation that would phase out federal liability limits for oil spills from single-hulled tankers and raise liability limits for oil spills overall. *See, e.g.*, Coast Guard and Maritime Transportation Act of 2006, Pub. L. No. 109-241, 120 Stat. 516, § 603. For additional discussion of Senator Lautenberg's efforts, see *Senator Lautenberg—Naval Architect*?, *supra* note 209.

the U.S., through regulatory or private litigation.[284] The movement from a private claims process conducted by BP for persons whose employment was adversely affected as a result of the Deepwater Horizon oil spill to a federal claims czar overseeing the claims—such as Kenneth Feinberg's Deepwater Horizon and 9/11 Claims processes[285]—suggests a model for claims resolution outside the court system at the election of the claimant.[286] Such claims processes are particularly important in cases in which there may be thousands of similarly situated claimants as well as those cases in which the claimant is unlikely to be able to access the technical expertise necessary to pursue his claims apart from the option of class actions. A rigorous claims procedure also would protect the entity experiencing the breach in the same manner that the alleged tortfeasor is protected by the "economic loss doctrine" barring recovery to claimants that cannot demonstrate actual damages.[287]

Payments data security is increasingly vital to the economy and to national security. After the 2010 Cyber Shock Wave simulation,[288] the former director of the National Security Agency during the Clinton Administration argued that the government needs more *capacity* to deal with cyber security events and strategies as well as the ability to work cooperatively with the private sector.[289] Only two of the federal bills analyzed in this Article—H.R. 2221 and S. 773—address strategic payments and non-payments security issues, such as malicious and strategic cyber attacks on infrastructure in the payments, utilities, and telecommunications areas in the U.S. This is accomplished through their grants of authority to order sequestration of systems that are compromised or that threaten other systems and infrastructures.[290] We also may need to impose stronger requirements on companies who have had more than one data security breach, such as ChoicePoint. And, finally, we can hope that

---

284. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 637 (7th Cir. 2007); Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 918 N.E.2d 36, 46–47, 50–51 (Mass. 2009) (denying recovery on a third-party beneficiary basis).

285. *See* Matthew Jaffe, *Ken Feinberg Named BP Oil Spill Escrow Pay Czar,* ABC NEWS, June 17, 2010, http://abcnews.go.com/Business/bp-gulf-oil-spill-ken-feinberg-appointedhead/story ?id=10933766; *see also* Laurel Brubaker Calkins, *BP Spill Claims Process Inadequate, Too Slow, Fishermen Tell Federal Judge,* BLOOMBERG NEWS, May 21, 2010, http://www.bloomberg.com/ news/2010-05-21/bp-spill-claims-process-inadequate-too-slow-fishermen-tell-federal-judge.html; Leigh Coleman, *BP Stalls Payments to Oil Spill Victims: Feinberg,* REUTERS, July 24, 2010, *available at* http://www.reuters.com/article/idUSTRE66N15020100724.

286. *See, e.g.*, Mireya Navarro, *Deal is Reached on Health Care Costs of 9/11 Workers,* N.Y. TIMES, Mar. 12, 2010, at A1 (describing option to pursue individual claims in court, which few heirs of the victims of the 9/11 attacks took).

287. *See, e.g.*, *In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498–99 (1st Cir. 2009); Banknorth, N.A., v. BJ's Wholesale Club, Inc., 394 F. Supp. 2d 283, 286–87 (D. Me. 2005).

288. *See* Mike McConnell, *To Win the Cyber-War, Look to the Cold War,* WASH. POST, Feb. 28, 2010, at B1.

289. *Id.*

290. Cybersecurity Act of 2009, S. 773, 111th Cong. § 18(2), (6) (2009).

multilateral organizations in the payments industry can play a stronger role than they have so far in framing for payments data protection functional equivalents of MARPOL's double-hulled vessels and other operational restrictions.

With the growing evidence of the cross-border implications of data spills, we would also do well to consider the benefits of international cooperation—recognizing, as Melissa Hathaway, former acting senior director for cyberspace for the National Security and Homeland Security Councils did, that the U.S. "'cannot succeed in securing cyberspace if it works in isolation.'"[291]

291. Steve Rangor, *Cyber Security: War Games or Mission Impossible?*, ZDNet (Apr. 27, 2009), http://www.zdnetasia.com/cybersecurity-war-games-or-mission-impossible-62053582.htm (quoting Hathaway's speech at the 2009 RSA Conference in San Francisco).