TESTING COMPLIANCE

BRANDON L. GARRETT* & GREGORY MITCHELL**

I
INTRODUCTION

Corporations must comply with a dizzying array of laws and regulations. To accomplish this complex task, corporations increasingly turn not just to the legal department and outside counsel but also to an in-house group composed of non-lawyer specialists who seek to educate and motivate personnel with respect to their obligations under the law and the corporation's code of conduct. The programs put in place aim to prevent a wide range of misconduct, from government bribery and financial fraud to environmental disasters and the creation of dangerous working conditions that jeopardize employees' physical and mental health.

Beyond the enormity of the task, what makes the compliance enterprise deeply uncertain and problematic is that the information generated by compliance efforts is simultaneously useful and dangerous. Even the most craven corporate officers and directors seek to prevent behaviors that may jeopardize employee performance, customer satisfaction, and stock prices. However, documenting problematic behaviors creates a record that may be used against the corporation in future administrative, criminal or civil proceedings, or may become the subject of a media exposé. Officers and directors, and the in-house compliance team, may sincerely hope the corporation's compliance programs are effective, but they may quite rationally avoid testing that hope. The end result will often be rational ignorance with respect to the effectiveness of corporate compliance programs. The hope that greater attention to compliance will reap benefits drives more resources toward compliance efforts, yet fears about what examining the effects of those efforts might reveal hinders validation of compliance programs. This dynamic creates a "compliance trap" that can ensnare corporations and regulators alike.[1]

This Article is also available online at http://lcp.law.duke.edu/.

* L. Neil Williams Professor of Law, Duke University School of Law and Director of the Wilson Center for Science and Justice, Duke University School of Law. Many thanks to Miriam Baer, Rachel Barkow, Sara Sun Beale, Sam Buell, Mihailis Diamantis, James Nelson, Veronica Root Martinez, Urska Velikonja, as well as all of the participants at the *Law and Contemporary Problems* Symposium at Duke Law in October 2019, and the participants at an incubator lunch at UVA Law School, for their invaluable comments on drafts.

** Joseph Weintraub–Bank of America Distinguished Professor of Law & Joseph C. Carter, Jr., Research Professor of Law, University of Virginia School of Law.

1. The problem that we label the "compliance trap" is different than that discussed by Christine Parker in an earlier article. Professor Parker discusses whether a lack of political support for a law's moral seriousness can cause underenforcement and a perception that enforcement of such a law is unfair.

In this Article, we explore ways out of this trap, focusing in particular on the regulatory conditions and mindsets that lead organizations and their watchdogs alike into the trap and make it so difficult to escape. We argue that hope-based compliance—a mentality that leads insiders and outsiders to assess compliance programs by examining how many resources organizations devote to the effort and whether the programs appear well-intentioned or comply with accepted best practices within an industry—predictably arises from the incentives and practices evident under current laws. Unfortunately hope-based compliance founded on good intentions and industry best practices provides little hope for effective self-regulation. We propose a set of legal reforms that would create the conditions for a move to evidence-based compliance.

Part II introduces the turn to internal compliance as a key element of government regulation and discusses the considerations that prevent organizations and their watchdogs from insisting on validated internal compliance. To make these considerations concrete and illustrate how they lead to more compliance programs without more validation of those programs, we then look at the compliance trap in the domains of (a) federal criminal prosecutions generally, (b) enforcement of the Foreign Corrupt Practices Act, (c) enforcement of the Bank Secrecy Act, and (d) enforcement of worker protection laws.

Part III then turns to data collected from public sources concerning compliance at Fortune 100 companies to assess how organizations present their compliance programs to the public. Consistent with the story told in Part II, we find that, while almost all Fortune 100 firms publicly disclose an extensive compliance apparatus, few publicly disclose any systematic efforts to assess the effects of their compliance programs.

Part IV examines the primary legal proposals advanced to try to incentivize organizations to undertake serious compliance efforts—an affirmative defense based on an organization's compliance efforts and a privilege for compliance-related information. We discuss the limits to these proposals, and then we build on these proposals to try to create legal conditions that will lead organizations and regulators out of the compliance trap. We discuss how a mandate for reporting on efforts to validate compliance, paired with a privilege focused on compliance validation data and a rule against use of mandated compliance reports in litigation, could extricate us from the compliance trap.

In Part V, we discuss how "compliance cartels"—coordinated compliance efforts among similarly-situated players within particular regulatory domains—

Christine Parker, *The 'Compliance' Trap: The Moral Message in Responsive Regulatory Enforcement,* 40 LAW & SOC'Y REV. 591, 591 (2006). The problem that is our focus is not compliance with the law broadly, but the reliance on internal compliance measures as a form of regulation. Our subject is related, however, because, as Parker develops, a regulator that avoids blunt deterrent fines by trying to create positive incentives for compliance risks efforts by industry to weaken the impact of enforcement on compliance. Parker suggests the only way to avoid that "trap" is to strengthen enforcers politically. *Id.* at 611. We, instead, suggest a more modest solution focusing on auditing and improvement of compliance requirements.

could efficiently produce shared information that would promote validated compliance within and across industries. We also provide concrete advice on how to go about testing compliance programs to overcome the problem that many in-house specialists and outside compliance consultants lack a validation mindset and fail to develop serious tests of implemented programs even if the will to validate exists.

Our concluding message is simple: implementation of compliance programs without rigorous validation of those programs constitutes nothing more than a hope that these programs will protect workers, stockholders, and the general public from organizational misconduct. That hope is likely to go unfulfilled, at a tremendous monetary and opportunity cost, in many cases. The compliance revolution must be empirically tested or should be considered a failed revolution.

II

THE RISE OF COMPLIANCE AND THE COMPLIANCE TRAP

Over the past three decades, an approach emphasizing compliance has entered the core of modern regulation, in areas ranging from civil rights and mass torts to environmental crimes and foreign bribery.[2] A range of federal agencies within the United States emphasize compliance when deciding whether to pursue enforcement actions, including the Department of Justice (DOJ), Environmental Protection Agency (EPA), Health and Human Services (HHS), and the Securities and Exchange Commission (SEC).[3] The compliance approach has also gone international: the Organization for Economic Cooperation and Development (OECD) recommends in-house compliance to combat bribery of foreign officials.[4] The DOJ has provided detailed guidance to evaluate corporate

2. *See, e.g.*, Stavros Gadinis & Amelia Miazad, *The Hidden Power of Compliance*, 103 MINN. L. REV. 2135, 2146 (2019) (noting that "U.S. Sentencing Guidelines [had] offered an up-to-ninety-five-percent reduction in penalties for companies" with effective compliance regimes "as early as 1991"); *see also* Brandon Garrett, *Structural Reform Prosecution*, 93 VA. L. REV. 856 (2007) (attributing the rise of compliance-based settlements to corporate misconduct in the 1990s).

3. *See, e.g.*, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, Exchange Act Release No. 44,969, 76 SEC Docket 296 (Oct. 23, 2001) [hereinafter SEC Report of Investigation] (asking, among factors informing SEC discretion, "[d]id the company adopt and ensure enforcement of new and more effective internal controls and procedures designed to prevent a recurrence of the misconduct?"); *see also* EPA Incentives For Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations, 65 Fed. Reg. 19,618, 19,618 (Apr. 11, 2000) [hereinafter EPA Incentives]("[I]ncentives that [the] EPA makes available for those who meet the terms of the Audit Policy include . . . a determination not to recommend criminal prosecution of the disclosing entity . . . .").

4. *See, e.g.*, ORG. FOR ECON. CO-OPERATION AND DEV. [OECD], RECOMMENDATION OF THE COUNCIL FOR FURTHER COMBATING BRIBERY OF FOREIGN PUBLIC OFFICIALS IN INTERNATIONAL BUSINESS TRANSACTIONS 6–8 (2009) [hereinafter OECD RECOMMENDATION], https://www.oecd.org/daf/anti-bribery/44176910.pdf [https://perma.cc/ME4F-2U74] (recommending that member states encourage "companies to develop and adopt adequate . . . compliance programmes . . . for the purpose of preventing and detecting foreign bribery"); *see also* OECD, GOOD PRACTICE GUIDANCE ON INTERNAL CONTROLS, ETHICS, AND COMPLIANCE 13–15 (Feb. 18, 2010) [hereinafter OECD GOOD PRACTICE GUIDANCE], https://www.oecd.org/daf/anti-bribery/44884389.pdf

compliance programs as a factor to consider when deciding what sanctions to pursue against alleged corporate wrongdoers.[5]

In those areas and many others, regulators, prosecutors, and private plaintiffs seek to not only punish a company for violations and compensate victims, but to encourage the organization to self-regulate. The compliance revolution starts from the premise that many organizations want to be good citizens and that these organizations are in the best position to determine how to comply with the goals set by lawmakers. Scholars advocating this "new governance" approach recognize that some organizations will exploit delegations of enforcement, but they reject reliance on active enforcement under a "command and control" regime as unrealistic given budgetary limits, and as inefficient given the difficulty of creating regulatory schemes in complex industries often subject to global competition and competing regulatory demands.[6]

Predictably, a compliance industry has mushroomed to counsel companies on how to fulfill the compliance mission. Yet by all accounts, it is a pervasive problem that we lack metrics to evaluate whether compliance programs—the focus of so much litigation and regulation—actually reduce underlying violations.[7] A combination of informational gaps, perverse incentives, and practical difficulties explain why compliance programs will often be better described as aspirational than validated means of achieving compliance.

First, public and private enforcement actions, by their nature, focus on revealed behavior rather than the quality of compliance efforts. Compliance measures may not earn a company credit from regulators if those measures fail to prevent violations no matter how sound those measures were—and private litigants often pursue civil claims regardless of the quality of compliance measures in place. Enforcement efforts suffer, in short, from an outcome bias (that is, negative outcomes or illegal behaviors elicit action, while positive outcomes and legal behaviors go unnoticed and elicit little or no response). In fact, corporations with sound compliance programs may be at greater risk of

---

[https://perma.cc/R7HN-X64B] (articulating "good practices for ensuring effective . . . compliance programmes . . . for the purpose of preventing and detecting foreign bribery").

5. *See, e.g.*, FRAUD SECTION, CRIM. DIV., U.S, DEP'T OF JUST., EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, 1 (2017) [hereinafter 2017 CORPORATE COMPLIANCE EVALUATION] (providing guidance on the "Filip Factors" that "prosecutors should consider in . . . determining whether to bring charges" against corporations); *see also* U.S. DEP'T OF JUST., CRIM. DIV., EVALUATION OF CORPORATE COMPLIANCE PROGRAMS 11 (2019), 1 [hereinafter 2019 CORPORATE COMPLIANCE EVALUATION] (providing guidance on "decisions as to whether, and to what extent, the corporation's compliance program was effective . . . for purposes of determining [*inter alia*] the appropriate (1) form of any resolution or prosecution"); U.S. Dep't of Just., Just. Manual § 9-28.300 (2018) (considering "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" in charging decisions).

6. *See, e.g.*, Orly Lobel, *New Governance as Regulatory Governance*, *in* OXFORD HANDBOOK OF GOVERNANCE 65, 68–77 (David Levi-Faur, ed. 2012) (describing the "scholarly critique" of command-and-control regulation); *id.*, at 72 ("In part, the literature describes new governance as a response to increased globalization.").

7. Parker, *supra* note 1, at 591.

litigation because effective programs should reveal areas of weakness to be exploited by regulators, plaintiff-side lawyers, and whistleblowers.[8]

Second, companies have no way to know, ex ante, which compliance measures will succeed in preventing violations, but gathering information on effectiveness can create internal problems apart from the external risks that come with possible disclosure of compliance-testing information. Considerable sums may be expended to validate a compliance program only to find that program is ineffective. Compliance departments operate under budgetary constraints that may make revamping compliance measures difficult, and the staff who put in place the ineffective programs may justifiably fear reputational harm from acknowledging the need for revamping. Moreover, serious validation efforts require that the conduct of employees be scrutinized for improprieties, a process that can create distrust and concern among those being scrutinized. A safer course for compliance teams is to focus on educating personnel about their general legal and ethical obligations, only focusing on actual behavior in the context of investigation of internal complaints, and then tweaking educational efforts to address behavioral gaps revealed by the investigations.

Third, without compliance data, outside decisionmakers, whether they be regulators, prosecutors, or judges, cannot easily distinguish cosmetic from effective compliance. Powerful regulators and prosecutors could insist that compliance be studied and audited, but they rarely insist that such care be taken, even as part of a plea agreement or conciliation agreement, much less that independent scientific researchers be given access to corporate data.[9] The fact that the persons with power to order validation efforts rarely do so reveals that the lack of validation is more than just an internal incentives problem—there is often little incentive for the regulators themselves to demand validation. Politically appointed regulators may be subject to industry capture, or they may see validation in the same way as corporate insiders: testing an imposed compliance program for effectiveness risks creating data, which may reveal wasted resources and lost opportunities associated with the imposed program. A much safer course is to tout the supposedly tough measures imposed on an organization through a settlement, without explaining how toughness was measured.

Fourth, non-governmental watchdogs lack the power to compel disclosure of the information needed to assess compliance programs unless legal action is taken, yet the threat of private litigation deters the creation of the very information needed to assess compliance programs. These non-governmental watchdogs, whether private attorneys general or issue-driven non-profits, understandably resist creation of privileges and safe havens designed to promote

8. Jennifer Arlen, *The Potentially Perverse Effects of Corporate Criminal Liability*, 23 J. LEGAL STUD. 833, 836–37 (1994).

9. *See* discussion *infra* Part. II.B.

internal scrutiny of compliance programs.[10] They fear that such protections will be exploited by firms to conceal wrongdoing without prompting meaningful change. Yet without such protections, many organizations will not voluntarily engage in self-critical scrutiny of their compliance programs absent legal mandates to do so.

Finally, the lack of compliance validation may be the product of a lack of imagination. Corporations ordinarily count on consumer markets and stock markets to keep score, but financial markets provide poor measures of corporate compliance efforts because licit conduct will be unremarkable and illicit conduct often remains latent for years. Serious validation efforts often require that new baselines and metrics be created to keep score; but designing and carrying out an empirical study to examine the efficacy of a compliance intervention can be difficult and time-consuming. Regulators and compliance team members, many of whom are lawyers or industry insiders, often do not have the empirical training needed to instill a validation mindset. As a consequence, companies and their watchdogs often focus on implementation rather than validation. In the following Subparts, we illustrate the compliance trap in operation across a variety of cases and contexts.

A. The Compliance Trap in Action: Siemens Corporation

The Siemens corporation settled the largest foreign bribery prosecution in history in 2008, having paid over $1.4 billion in bribes to government officials around the world for over a decade.[11] Siemens ultimately pleaded guilty to violations of the Foreign Corrupt Practices Act (FCPA) and agreed to pay $1.6 billion in fines to American and German prosecutors, as well as agreeing to four years of supervision by two corporate monitors.[12] The monitors were directed to conduct an initial review of Siemens's anti-corruption compliance program and prepare an initial assessment, followed by three annual reports, with a final report addressing whether the compliance program was "reasonably designed and implemented" to "detect and prevent violations."[13] The monitors were given sweeping powers to access Siemens's documents and records, conduct on-site

10. *See, e.g.*, Joseph E. Murphy, *Policies in Conflict: Undermining Corporate Self-policing*, 62 RUTGERS U.L. REV. 421, 450–51 (2017) (discussing opposition to extension of the self-evaluative privilege to compliance programs); PUB. CITIZEN, CORPORATE IMPUNITY 6 (2018) (describing a shift towards rewarding self-reporting as a "softening" of corporate enforcement), https://www.citizen.org/wp-content/uploads/corporate-enforcement-public-citizen-report-july-2018.pdf [https://perma.cc/8RA6-QDPR].

11. Press Release, U.S. Dep't of Just., Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations and Agree to Pay $450 Million in Combined Criminal Fines (Dec. 15, 2008), https://www.justice.gov/archive/opa/pr/2008/December/08-crm-1105.html [https://perma.cc/EH2W-X7WP].

12. *Id.*

13. Notice Regarding Corporate Monitorship ¶¶ 4–7, United States v. Siemens Aktiengesellschaft, No. 08-367 (D.D.C. Dec. 18, 2012), ECF No. 23; *see also* Plea Agreement ¶ 12, *Siemens Aktiengesellschaft*, No. 08-367 (D.D.C. Dec. 15, 2008), ECF No. 14.

inspections, interview employees, and test compliance systems.[14] That monitorship was, by all accounts at the time, quite successful, and the company emerged from that period of oversight lauding its transformation and adoption of a sweeping new compliance program designed to prevent corruption in its global operations.[15]

In 2014, a group of reporters asked that the reports of Siemens's corporate monitors be made public.[16] Their Freedom of Information Act (FOIA) request was opposed by the DOJ, stating that the monitor reports contained sensitive information and that making such documents public might harm the ability of monitors to gather candid and accurate information. These efforts could be undermined since the monitor reports contained "detailed descriptions of Siemens' compliance programs and business operations."[17]

The DOJ also made a very different argument, however, endorsing an objection raised by Siemens itself, after Siemens and a monitor both intervened in the litigation.[18] Disclosing this information would provide a "free roadmap" to competitors as to "what works" and "how to build an effective compliance program" without the "extraordinary costs" that Siemens incurred.[19] Perhaps Siemens would have good reasons to protect its investment in compliance. It is much harder to understand why the DOJ would not want a company convicted of serious crimes to have to share such information if it could help other companies to effectively prevent such corruption offenses. Ultimately, the federal district judge agreed that much of the sought-after material, including the monitor work plans and reports, was "plainly commercial," which would provide a "free roadmap" to others in industry," and therefore exempt from FOIA. However, the court also ordered the company to provide reports and documents in camera for further review.[20]

The reasons that the DOJ offered in this high-profile litigation for keeping the workings of a supposedly highly effective compliance program non-public crystallize the problem we call the "compliance trap." Enforcers should want

14. Notice Regarding Corporate Monitorship, *supra* note 13, ¶ 7.

15. SIEMENS, COMPLIANCE PROGRAM @ SIEMENS 5 (2010), https://www.oecd.org/countries/iraq/44927648.pdf [https://perma.cc/B2F7-3TY9] (claiming in a report to OECD that Siemens "is now seen as an industry benchmark in compliance and sustainability").

16. Complaint for Injunctive Relief ¶¶ 1–2, 100Reporters LLC v. U.S. Dep't of Just., 248 F. Supp. 3d 115 (No. 1:14-cv-01264) (D.D.C. 2016), 2014 WL 3720435. Those reporters have made available online a series of documents from the FOIA litigation. *See, e.g.*, Adam Dobrik, *DOJ's Siemens Compliance Monitor Position 'Troubling'*, GLOB. INVESTIGATIONS REV. (Aug. 24, 2016), https://globalinvestigationsreview.com/article/jac/1067691/doj's-siemens-compliance-monitor-position-"troubling" [https://perma.cc/79PS-JC6N].

17. Def. U.S. Dep't of Just.'s Combined Reply in Support of its Motion for Summary Judgment and Opposition to Plaintiff's Cross-Motion for Summary Judgment at 25, *100Reporters LLC*, 248 F. Supp. 3d 115 (No. 1:14-cv-1264), 2016 WL 10006770 [hereinafter Defendant's Combined Reply].

18. *See 100Reporters LLC*, 248 F. Supp. 3d at 126.

19. Defendant's Combined Reply, *supra* note 17, at 15. Separately, the DOJ argued that "Disclosure would also chill vigorous discussions within DOJ regarding the adequacy of monitors' efforts, thereby undermining the effectiveness of such monitorships in addressing corporate crime." *Id.* at 10.

20. *100Reporters LLC*, 248 F. Supp. 3d at 134, 140, 166–67.

companies to share sound compliance practices to improve standards in industry generally. Individual companies, however, have incentives not to share information about compliance failures, lest they risk liability. Nor do companies have strong incentives to share information about compliance successes, lest their competitors use their strategies too. Yet regulators should want all companies in industry to use effective techniques to prevent crimes from occurring. Rather than address this problem, regulators and enforcers like the DOJ, as we will explore, have exacerbated the problem by failing to incentivize sharing compliance strategies, and even encouraging companies to keep such information to themselves.

The notion that the compliance function should be handled not just by the legal department within a company, but by compliance specialists, is relatively new. Traditionally, compliance with law was the subject assigned to the general counsel of a company, or to compliance professionals that reported to the general counsel.[21] Today, there is a far more diverse set of practices among public companies, with some companies centralizing compliance with the general counsel, while others view at least some types of compliance with legal and ethical standards as a separate function.[22] Prosecutors and regulators have sometimes required that companies separate the compliance function and create new compliance positions reporting to the board and not just to the general counsel. Scholars have debated whether structuring compliance separately within a firm is a good or bad idea.[23]

Over the past three decades, compliance has entered the core of modern regulation, in areas ranging from civil rights, to mass torts, to environmental crimes, and foreign bribery. A range of federal agencies emphasize compliance when deciding whether to pursue enforcement actions, including the EPA, HHS-OIG, and the SEC.[24] The United States Sentencing Guidelines (Guidelines) reward convicted companies that maintain "effective" compliance programs.[25] The Patient Protection and Affordable Care Act (colloquially called Obamacare) requires that health care providers maintain effective compliance and ethics programs.[26] The Delaware Court of Chancery, in 1996, held that a corporate

21. Michele DeStefano, *Making a Culture of Compliance: Why Departmentalization May Not Be the Answer*, 10 HASTINGS BUS. L. J. 71, 110 n.98 (2014).

22. *Id.* at 100–01 nn.115–20.

23. *See*, *e.g.*, *id.* at 170 (arguing that "informal norms and networks, human ethics, and motivation" are more critical than official compliance structures); *see also* Tanina Rostain, *General Counsel in the Age of Compliance: Preliminary Findings and New Research Questions*, 21 GEO. J. LEGAL ETHICS 465, 469 (2008) (arguing that complex modern regulations require extensive non-legal skillsets of compliance professionals); Donald C. Langevoort, *Getting (Too) Comfortable: In-house Lawyers, Enterprise Risk and the Financial Crisis*, 2012 WIS. L. REV. 495, 500, 502, 518 (2012) (observing that "the right outcome depends on the particular firm's history, incentives, and culture").

24. *See* sources cited *supra* note 3.

25. U.S. SENT'G GUIDELINES MANUAL § 8C2.5(f) (U.S. SENT'G COMM'N 2018).

26. *See* Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, § 6102 (2010) (mandating that skilled nursing facilities establish "compliance and ethics program[s] that [are] effective in preventing and detecting criminal, civil, and administrative violations").

director may be held liable for failure to implement adequate compliance.[27] The OECD has recommendations for compliance to combat bribery.[28] The DOJ provided detailed guidance in 2017 designed to evaluate corporate compliance programs, with this guidance updated in 2019.[29]

This turn to internal compliance promises the prevention of unlawful behavior without the need for costly and risky public enforcement actions that, if unsuccessful, may undercut a law's deterrence effects. Yet we presently have little reason to believe this promise is being fulfilled. As also illustrated by the Siemens case, the information that the public needs to assess internal compliance programs is often lacking, with organizations understandably reluctant to divulge that information, and that reluctance is sometimes abetted by regulators and prosecutors.

Under current DOJ guidelines, when deciding whether to take action against a company for violation of federal law, prosecutors should gather information on the methodology used by the company "to identify, analyze, and address the particular risks it faced" and the "information or metrics . . . the company collected and used to help detect the type of misconduct in question."[30] If no such information exists, then presumably the company undertook no serious effort to identify and mitigate compliance risks, suggesting that compliance efforts, either intentionally or unintentionally, were more cosmetic than real."[31] But presently, the DOJ does not require that its assessments of a company's compliance and risk mitigation programs be made public. Until we understand why organizations and those charged with their oversight fail to engage in the empirical studies needed to validate compliance programs or fail to make public such information when it exists, we cannot begin to avoid the compliance trap.

B. The Rise of Unvalidated Corporate Compliance

The goal of this Part is to describe how, in four important areas, compliance is central to enforcement efforts but remains ill-defined and lacks incentives to validate or audit the effectiveness of compliance. In particular, we discuss the role of internal compliance and how it is treated in the context of the federal prosecution and sentencing of corporations generally and specifically under the FCPA, enforcement actions under the Bank Secrecy Act, and sexual harassment cases filed under Title VII.

---

27. *In re* Caremark Int'l., Inc. Derivative Lit., 698 A.2d 959, 970 (Del. Ch. 1996).

28. OECD RECOMMENDATION, *supra* note 4; OECD GOOD PRACTICE GUIDANCE, *supra* note 4.

29. *See* 2017 CORPORATE COMPLIANCE EVALUATION, *supra* note 5, at 11; *see also* Dep't of Just., Just. Manual § 9-28.300 (2018).

30. *See* 2017 CORPORATE COMPLIANCE EVALUATION, *supra* note 5, at 4.

31. Kimberly D. Krawiec, *Cosmetic Compliance and the Failure of Negotiated Governance*, 81 WASH. U. L. Q. 487, 500–11 (2003).

1. Compliance in Corporate Prosecutions

Compliance lies at the core of the modern approach towards corporate crime that has evolved over the past two decades. The U.S. Sentencing Guidelines adopted an approach that was the first to make corporate compliance salient. When the original federal Guidelines took effect in 1987, they did not include any separate rules for the sentencing of corporations or other types of organizations. The United States Sentencing Commission (Commission) studied the matter further and decided to draft separate Organizational Sentencing Guidelines (Organizational Guidelines), which took effect in 1991.[32] The Guidelines, including the Organizational Guidelines, are now advisory after *United States v. Booker*[33]; however, judges still begin their work by calculating the range the Guidelines recommend, and often stay within that range.[34]

As the Commission designed the Organizational Guidelines, it ultimately rejected a pure deterrence approach towards punishing organizations, deciding that it was too hard to estimate what fine it would take to prevent a company from re-offending or hiding misconduct.[35] Using fines to punish a company raises real complications. Even large fines may have no effect if companies can pass on costs to shareholders or customers, while the managers responsible remain unaffected.[36] The Commission also wanted to reward companies that appeared to try hard to prevent, detect, and report wrongdoing. After all, without a strong compliance defense, as Professors Jennifer Arlen and Reinier Kraakman have argued, a company will have no incentive to prevent crime, uncover wrongdoing, and report it to the authorities.[37] Many types of business crimes, such as fraud schemes that deceive victims, may never come to light unless companies themselves uncover what went wrong.

The approach that the Organizational Guidelines adopted rewards a company that, among other things, has an "effective compliance and ethics program."[38] Companies with "good" culpability have points taken away and can

32. Cindy R. Alexander, Jennifer Arlen & Mark A. Cohen, *Regulating Corporate Criminal Sanctions: Federal Guidelines and the Sentencing of Public Firms,* 42 J.L. & ECON., 393, 394 (1999).

33. *See* United States v. Booker, 543 U.S. 220, 266–67 (2005) (holding mandatory sentencing guidelines unconstitutional under the 6th Amendment).

34. *See* 2019 U.S. SENT'G COMM'N Q. DATA REP. 11 tbl.8, https://www.ussc.gov/sites/default/files/pdf/research-and-publications/federal-sentencing-statistics/quarterly-sentencing-updates/USSC-2019_Quarterly_Report_Final.pdf [https://perma.cc/R48A-LYFJ] (finding judges stay within Guideline ranges in more than 50% of sentences).

35. *See* Jeffrey S. Parker, *Criminal Sentencing Policy for Organizations: The Unifying Approach of Optimal Penalties*, 26 AM. CRIM. L. REV. 513, 555 (1989) (reporting that deterrence advocates on the Commission were unable to establish an empirical justification for guidelines based on a theory of deterrence); *see also* Ilene H. Nagel & Winthrop M. Swenson, *The Federal Sentencing Guidelines for Corporations: Their Development, Theoretical Underpinnings, and Some Thoughts About Their Future*, 71 WASH. U. L.Q. 205, 219 (1993) (characterizing the available empirical evidence as "bordering on mere assumptions").

36. Jennifer Arlen & Reinier Kraakman, *Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes*, 72 N.Y.U. L. REV. 687, 699 (1997).

37. *Id.*

38. *See* U.S. SENT'G GUIDELINES MANUAL § 8C2.5(f) (U.S. SENT'G COMM'N 2018).

have fines cut in half or even more.[39] Two factors in particular can reduce the fine: (1) evidence of an effective compliance and ethics program and (2) evidence of a desire to end the misconduct, as indicated by self-reporting, cooperation, or acceptance of responsibility.[40]

What counts as an effective compliance program? The Guidelines state that a compliance program must be "reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct."[41] In 2003, the Commission moved this description of effective compliance from footnoted "commentary" into the guidelines, to highlight its importance, and added details about what should be in place, like training, monitoring, anonymous reporting of misconduct, and evaluation.[42] And in 2010, the Commission amended the rule to make clear that, even if a high-level employee committed a crime, the company may still receive a reduced sentence if it presents evidence of an effective compliance program.[43]

It is hard to know what evidence is needed to meet this "effective compliance" test, however, because only a handful of companies have ever received credit under the effective compliance factor. In fiscal years 2009 through 2012, for example, the Commission reported no companies as receiving credit under this factor Presently, it is impossible to know whether so few companies receive credit under the effective compliance factor because few companies have effective compliance programs, because prosecutors and judges reject the evidence companies submit on this factor, or because other factors drive the outcome in a case.

Courts can also order a convicted company to adopt stronger compliance protections as part of the company's sentence. The Commission amended the guidelines to encourage probation to supervise compliance. The court may "employ appropriate experts" to review a compliance program.[44] The company can be ordered to allow unannounced visits by probation officers to examine books or records (or by an expert appointed by the judge for such purposes), and to make employees available for "interrogation."[45] Nevertheless, corporate probation is typically unsupervised.[46]

The emphasis on compliance in the Guidelines may have had a greater impact by influencing prosecutors, who now offer alternatives to prosecution (in the form of deferred prosecution and non-prosecution agreements) to corporations

39. *Id.* § 8C2.6.

40. *Id.* § 8C2.5(f)–(g).

41. *Id*. § 8B2.1(a)(2).

42. *Id.* § 8B2.1(a)(2), (b)(2); U.S. SENT'G COMM'N, REPORT OF THE AD HOC ADVISORY GROUP ON THE ORGANIZATIONAL GUIDELINES (2003).

43. U.S. SENT'G GUIDELINES MANUAL § 8C2.5(3).

44. *Id.* § 8D1.4 cmt. n.1.

45. *Id.* § 8D1.4(5).

46. BRANDON L. GARRETT, TOO BIG TO JAIL: HOW PROSECUTORS COMPROMISE WITH CORPORATIONS 3 (2016).

that self-report, cooperate, and adopt effective compliance programs.[47] A company can avoid indictment and have its case stayed for a period of time on the judge's docket while it complies with a deferred prosecution agreement, or it can avoid a court filing at all by complying with the terms of a non-prosecution agreement.[48] In general, these agreements require the firm to pay a monetary penalty, acknowledge responsibility, admit inculpatory facts, agree to cooperate in any additional investigations, implement compliance improvements, and permit prosecutorial oversight.[49]

In 1999, under then-Deputy Attorney General Eric Holder, the DOJ issued its first memorandum providing guidelines for corporate prosecutions.[50] The deferred prosecution approach was more firmly set out in 2003 in a set of revised DOJ guidelines, or "Principles," for the prosecution of organizations contained in the U.S. Attorneys' Manual.[51] These Principles were popularly called the "Thompson Memo," after Larry Thompson, the Deputy Attorney General at the time who authored the guidelines.[52] The DOJ emphasized at the inception that compliance was a central goal of the new approach, asserting that this approach would make prosecutors "a force for positive change of corporate culture, alter corporate behavior, and prevent, discover, and punish serious [white collar] crime."[53] The Principles state that the existence and "effectiveness of the corporation's [pre-existing] compliance program" is a factor in deciding whether to prosecute a company in the first place.[54] The Principles add that "the existence of a compliance program is not sufficient, in and of itself, to justify not charging

47. For a discussion of the increasing emphasis on information and compliance in charging decisions, see Veronica Root Martinez, *The Government's Prioritization of Information Over Sanction: Implications for Compliance*, 83 LAW & CONTEMP. PROBS., no. 4, at 87, 102–06 (2020).

48. Cindy R. Alexander & Mark A. Cohen, *The Evolution of Corporate Criminal Settlements: An Empirical Perspective on Non-Prosecution, Deferred Prosecution, and Plea* Agreements, 52 AM. CRIM. L. REV. 537, 544–45 (2015)

49. *See* Cindy R. Alexander, Yoon-Ho Alex Lee, *Non-Prosecution of Corporations: Toward A Model of Cooperation and Leniency*, 96 N.C. L. REV. 859, 870 (2018) ("[S]ettlement agreements often contain provisions that commit the company to reforms, depending on the type of misconduct."); Miriam H. Baer, *Three Conceptions of Corporate Crime (and One Avenue for Reform)*, 84 LAW & CONTEMP. PROBS., no. 4, at 1, 2 (2020) ("This [deferred prosecution agreement] may require any number of commitments including the payment of fines, oversight by monitors, compliance and governance changes, and promises to alter or disband certain operational practices.").

50. Memorandum from Eric H. Holder Jr., Deputy Att'y Gen., to All Component Heads and U.S. Att'ys on Bringing Criminal Charges Against Corporations (June 16, 1999), https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2010/04/11/charging-corps.PDF [https://perma.cc/J6RH-QVD3].

51. Memorandum from Larry D. Thompson, Deputy Att'y Gen., to Heads of Dep't Components & U.S. Att'ys on Principles of Federal Prosecutions of Business Organizations (Jan. 20, 2003) [hereinafter *Thompson Memo on Business Organizations*] https://web.archive.org/web/20030608114303/http://www.usdoj.gov/dag/cftf/corporate_guidelines.htm [https://perma.cc/J6N7-S3VJ]; U.S. Dept. of Just., U.S. Att'ys' Manual § 9-28.800 (2008). The U.S. Attorneys' Manual is now the Justice Manual.

52. *Thompson Memo on Business Organizations*, *supra* note 51.

53. U.S. Dep't of Just., Just. Manual § 9-28.200A (2018).

54. *Id.* at § 9-28.300(5).

a corporation for criminal misconduct undertaken by its officers, directors, employees, or agents."[55] However, the Principles then add:

> The Department has no formulaic requirements regarding corporate compliance programs. The fundamental questions any prosecutor should ask are: Is the corporation's compliance program well designed? Is the program being applied earnestly and in good faith? Does the corporation's compliance program work?[56]

Finally, the Principles note that prosecutors should try to assess whether the program is just a "paper program," and should consider "whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts."[57] Those additional caveats highlight how loosely prosecutors appear to regulate compliance in practice. Prosecutors do not seem to follow the approach of the Organizational Guidelines, which emphasize that no compliance program is "effective" if the company does not "evaluate periodically" its effectiveness.[58] The first author has found that in practice, prosecutors do not routinely insist that a company assess or evaluate compliance. Between 2001 and 2012, few deferred and non-prosecution agreements require that the company evaluate the effectiveness of its compliance program to find out if it is really working or not.[59] While the agreements typically say that the compliance program must be "clearly articulated" and "rigorous" and "effective," those terms are not defined.[60]

Perhaps as a result, compliance itself may not commonly be evaluated carefully. According to one industry survey in 2013, less than half of companies conduct periodic compliance assessments.[61] Senator Edward Kennedy, who sponsored the legislation that gave birth to the Guidelines, pointed out that the key to sentencing organizations was that prosecutors and judges "must be able to tell the difference between sincere and cosmetic compliance efforts."[62] Prosecutors have perhaps more power than any other government actor to demand compliance reforms and supervise their implementation. Yet Judge Rakoff, Senior Judge of the United States District Court for the Southern District of New York, has observed that what prosecutors now do largely consists of

---

55. *Id.* at § 9-28.800.

56. *Id*.

57. *Id*.

58. U.S. SENT'G GUIDELINES MANUAL § 8B2.1(b)(5)(B) (U.S. SENT'G COMM'N 2018). Notably, however, how those assessments are to be done is not defined in the Guidelines.

59. GARRETT, *supra* note 46 at 175 fig.7.1 (showing that only 54 of 254, or 21% of agreements studied contained any such requirement).

60. *Id.*

61. Sue Reisinger, *ACC Study Sees Compliance Moving Out of the GC's Office*, CORP. COUNSEL (Oct. 15, 2013), https://www.law.com/corpcounsel/almID/1202623517245&rss=rss_cc_mostvi/ [https://perma.cc/TT5R-KXBK].

62. Senator Edward M. Kennedy, Keynote Address at the United States Sentencing Commission Symposium: Corporate Crime in America: Strengthening the "Good Citizen" Corporation (Sept. 7, 1995).

"imposing internal compliance measures that are often little more than window-dressing."[63]

Despite the priority placed on effective compliance by the Organizational Guidelines, there is little evidence that prosecutors rigorously try to assess whether compliance was working when misconduct occurred or whether compliance reforms that they order a company to adopt have positive effects.[64] In a 2014 study of corporate federal prosecutions agreements, the first author found that sixty-three percent of publicly available agreements required compliance reforms.[65] The study further showed that sixty-four percent of the agreements cited to steps already in place to improve compliance, and more than a quarter cited to compliance reforms required by regulators.[66] Most agreements did not require firms to hire monitors to evaluate compliance programs.[67] While the Guidelines say that no compliance program is "effective" if the company does not "evaluate periodically" its effectiveness,[68] prosecutors do not normally insist on such an evaluation.[69]

Indeed, for some time, the DOJ resisted recommendations from scholars and the Government Accountability Office to develop "performance measures."[70] The DOJ's stance on performance measures ostensibly began to change in late 2015, when the DOJ retained a Compliance Counsel Expert, in order to refocus efforts to assess corporate compliance in criminal investigations.[71] The new expert would "help prosecutors develop appropriate benchmarks for evaluating corporate compliance and remediation measures and communicating with stakeholders in setting those benchmarks."[72] In February 2017, the DOJ's Fraud Section produced detailed new guidance, titled "Evaluation of Corporate Compliance Programs,"[73] which the DOJ updated and adopted in 2019.[74] These guidelines were designed as a supplement to the existing organizational charging guidelines, which already stated that the "existence and effectiveness" of a

63. Jed S. Rakoff, *The Financial Crisis: Why Have No High-Level Executives Been Prosecuted?*, N.Y. REV. BOOKS (Jan. 9, 2014), https://www.nybooks.com/articles/2014/01/09/financial-crisis-why-no-executive-prosecutions/ [https://perma.cc/RYZ8-M7MK].

64. GARRETT, *supra* note 46, at 48.

65. *Id.*

66. *Id.*

67. *See id.* at 174 ("[O]nly 25 percent of the deferred prosecution and non-prosecution agreements entered into between 2001 and 2012 required a monitor (65 of 255 agreements).").

68. U.S. SENT'G GUIDELINES MANUAL § 8B2.1 (U.S. SENT'G COMM'N 2018).

69. GARRETT, *supra* note 46, at 48.

70. U.S. GOV'T ACCOUNTABILITY OFF., GAO-10-110, CORPORATE CRIME: DOJ HAS TAKEN STEPS TO BETTER TRACK ITS USE OF DEFERRED AND NON-PROSECUTION AGREEMENTS, BUT SHOULD EVALUATE EFFECTIVENESS 20 (2009), https://www.gao.gov/assets/300/299781.pdf [https://perma.cc/7MYB-2S7D].

71. Press Release, U.S. Dep't of Just., New Compliance Counsel Expert Retained by the DOJ Fraud Section (2015), https://www.justice.gov/criminal-fraud/file/790236/download [https://perma.cc/977C-XSG2] .

72. *Id.*

73. 2017 CORPORATE COMPLIANCE EVALUATION, *supra* note 5.

74. 2019 CORPORATE COMPLIANCE EVALUATION, *supra* note 5.

compliance program were relevant to charging decisions, as well as a corporation's remedial efforts to implement or improve its compliance.[75] The guidelines emphasize there should be "an individualized determination in each case."[76]

Of greatest interest here, the analysis emphasizes far more than any prior guidance the need to conduct risk assessments and audit the effectiveness of compliance, using several types of methods. The guidance emphasizes asking what tools the company uses to engage in "root cause analysis of the misconduct at issue."[77] The guidance does not address what risk assessment tools or data gathering or methods are effective in any given type of industry; it merely highlights the need for a data-driven analysis to ensure that compliance is working.

This DOJ guidance includes as relevant the collection of critical data and analysis of its implications. However, the guidance does not include any statement that such data collection is to be rewarded. Instead, much of the focus is on the culture of compliance, demonstrated commitment to compliance, training on compliance, resources for compliance, and due diligence regarding compliance in the mergers and acquisitions context. The guidance is a step forward for the DOJ, and each of those factors may correspond with a strong compliance program. However, indicia of investment in compliance is no substitute for empirical validation of a compliance program. The important point for our purposes is to emphasize that the legal framework exists for encouraging organizations to validate their compliance programs because such validation should be taken into account in charging and sentencing decisions. Unfortunately, available public data suggests that prosecutors and judges fail to utilize this framework consistently to create an expectation on the part of organizations that validated compliance programs, and only validated compliance programs, will be rewarded should the firm be prosecuted.

2. FCPA Prosecutions

The FCPA[78] provides a related case in point. The Act prohibits certain payments and gifts to foreign government officials and mandates record-keeping and internal controls designed to detect and prevent corrupt behavior.[79] Although enacted in 1977, enforcement of the FCPA exploded in the twenty-first century.[80] The statute itself makes compliance relevant to liability, since it prohibits not just bribery but also the failure to maintain accurate books and records and a "system of internal accounting controls sufficient to provide

75. 2017 CORPORATE COMPLIANCE EVALUATION, *supra* note 5, at 1.

76. *Id.*; 2019 CORPORATE COMPLIANCE EVALUATION, *supra* note 5, at 1.

77. 2019 CORPORATE COMPLIANCE EVALUATION, *supra* note 5, at 16.

78. Foreign Corrupt Practices Act of 1977, Pub. L. No. 95-213, 91 Stat. 1494 (codified as amended at 15 U.S.C. §§ 78m, 78o, 78dd-1 to -3 (2012)).

79. 15 U.S.C. § 78m.

80. Lucinda A. Low, *Ethics, Extraterritorial Anticorruption Laws and Anti-Money Laundering Laws*, 51 ROCKY MT. MIN. L. FOUND. 3-1, 3-51–52, (2005).

reasonable assurances" that transactions are conducted properly.[81] Compliance has been important in the practice of FCPA prosecutions, with prosecution agreements typically providing that compliance and ethics programs must be evaluated periodically and typically providing for the appointment of monitors.[82]

Designing a program to prevent illegal payments can be a difficult task for a multinational company with thousands of employees operating in many countries around the world, and with foreign subsidiaries engaging in millions of transactions that could each, standing alone, subject the entire company to prosecution. Having a clear company policy against payments of bribes, training on that policy, and procedures to approve payments with third parties are an important starting place.[83] However, in some parts of the world, practices may be entrenched with the custom that gifts and bribes are considered an obligatory and ordinary part of doing business.[84] How one audits transactions to be sure that they are not a cover for an illicit bribe is difficult, but one can spot-check transactions, identify certain red flags for improper payments, and carefully investigate potentially problematic transactions.

Many in industries affected by the FCPA hoped for additional guidance on compliance efforts when the DOJ released in 2012 a book-length guide to the FCPA.[85] However, that guidebook said little about what makes for a "strong compliance program," aside from stating that risk assessment is "fundamental" and noting that "targeted audits" can be used to test compliance procedure.[86] More recently, in April 2016, the DOJ Criminal Fraud Division announced an innovative pilot program in FCPA cases, in which corporations would receive different degrees of leniency based on three overarching factors: (a) voluntary self-disclosure, (b) full cooperation, and (c) timely and appropriate remediation.[87] That third category encompasses implementation of "an effective compliance program" as part of remediation.[88] But the criteria used to assess compliance are general, such as whether the company has established a "culture of compliance," whether it dedicates sufficient resources to compliance, and the

81. 15 U.S.C. § 78m(b)(2).

82. GARRETT, *supra* note 46, at 75.

83. For example, practice guides making detailed recommendations concerning elements of anti-bribery compliance programs. *See, e.g.*, Low, *supra* note 80 (explaining that FCPA compliance is best served by programs with a company compliance policy, due diligence procedures for third-party relationships and, among others, personnel training).

84. For explication on the heterogeneity of the cultural construct of bribery, see generally Steven R. Salbu, *The Foreign Corrupt Practices Act as a Threat to Global Harmony*, 20 MICH. J. INT'L L. 419, 422–26 (1999).

85. *See generally* CRIM. DIV., U.S. DEP'T OF JUST. & ENF'T DIV., U.S. SEC. & EXCH. COMM'N, A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT (2012) [hereinafter FCPA RESOURCE GUIDE], https://www.justice.gov/criminal-fraud/file/1292051/download [https://perma.cc/7JLA-VDGX].

86. *Id.* at 58, 62.

87. CRIM. DIV., U.S. DEP'T OF JUST., THE FRAUD SECTION'S FOREIGN CORRUPT PRACTICES ACT ENFORCEMENT PLAN AND GUIDANCE 1–3 (2016), https://www.justice.gov/archives/opa/blog-entry/file/838386/download [https://perma.cc/FDJ5-FJLZ].

88. *Id.* at 3.

"independence of the compliance function."[89] The guidance does include a statement that "auditing of the compliance program to assure its effectiveness" is a relevant factor as well as having "effective risk assessment."[90]

Practitioners have complained the guidance leaves companies uncertain about how they should go about the task of assessing their risks and ensuring that compliance is sufficiently effective.[91] And what it means to possess a "culture of compliance" is far from clear. Larry Thompson, the author of the Thompson Memo, recently commented that "there is so much uncertainty in FCPA enforcement that *the risk cannot even be intelligently evaluated.*"[92] Most important for our purposes, companies do not know whether they must evaluate, audit, or "stress test" their compliance programs, and if so what the results will be if they uncover weaknesses or outright FCPA violations. Instead, the DOJ has merely indicated through guidance that risk assessment and auditing are useful.[93] In particular prosecution agreements, the DOJ has noted that some "targeted" audits are useful, and the DOJ has asked companies and monitors to periodically review compliance, without specifying how to do so.[94]

The DOJ could specify how effective risk assessments or auditing should be conducted. The DOJ could make public monitor reports describing how to build an effective compliance program. The DOJ could clearly reward collection of self-critical data that would empower risk assessments and auditing of compliance. The DOJ could encourage companies to conduct experiments—trying one type of program for one subsidiary and another type for a different subsidiary, and then using audits to test which performed better. Not only would greater detail on how to audit compliance provide more notice to companies, but it would allow the DOJ to more carefully assess whether a company should be prosecuted or be allowed to terminate a deferred or non-prosecution agreement. Nevertheless, the DOJ has avoided development of more detailed compliance

89. *Id.*

90. *Id.*

91. *See* Ashby Jones, *Legal Maze's Murkiest Corners*, WALL ST. J. (Dec. 22, 2012), https://www.wsj.com/articles/SB10001424127887324731304578193950561507398 [https://perma.cc/Y25M-Z8AH] (describing in-house counsel for large companies calling the FCPA as one of the top areas of legal uncertainty they face); *Foreign Corrupt Practices Act Assessment: Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 38 (2011) (testimony of George J. Terwilliger) ("When faced with that uncertainty, companies sometimes forgo deals they could otherwise do, take a pass on contemplated projects or withdraw from ongoing projects and ventures. Companies making such decisions are not doing so because they are generally risk-averse. They are doing so by the simple reasoning that the risk of non-compliance, as defined by the statute and those charged with its enforcement, cannot be calculated with sufficient certainty.").

92. Larry D. Thompson, *In-Sourcing Corporate Responsibility for Enforcement of the Foreign Corrupt Practices Act*, 51 AM. CRIM. L. REV. 199, 207 (2014) (emphasis in original). Thompson added, "The best face that can be put on the situation is that the Justice Department itself does not understand *its own need* to provide meaningful guidance to help well-intentioned, would-be law-abiding corporations navigate the FCPA minefield." *Id.* at 213.

93. FCPA RESOURCE GUIDE, *supra* note 85, at 66.

94. GARRETT, *supra* note 46, at 75.

guidance and has not used FCPA agreements as a vehicle for evaluating corporate compliance data to test which types of procedures work best.

Again, as with federal prosecutions of corporations generally, the legal environment created under the FCPA properly focuses on *effective* compliance and enables prosecutors to develop guidance on how to both assess compliance and reward it. But the DOJ and U.S. Attorneys have failed to provide the guidance and incentives needed to develop and reward validated compliance programs.

3. The Bank Secrecy Act (BSA)

In some legal domains, statutes not only require compliance but also require that companies use certain methods to audit or assess their compliance with the statute or associated regulations. For instance, the BSA requires that banks and other financial institutions file currency transaction reports (CTRs) for transactions involving more than $10,000 in cash in a single business day,[95] and Suspicious Activity Reports (SARs) for suspicious transactions over $5,000.[96] Banking transactions are usually not conducted with cash at a teller's window but are now chiefly electronic. In a typical year, almost 15 million currency transaction reports are filed, and almost 1.5 million suspicious activity reports are filed.[97] Since 2002, the BSA as amended by the Patriot Act, has required that banks create anti-money laundering (AML) programs to review reports to ensure no transactions violated the law.[98] The BSA and implementing regulations have required four key components from these programs: (1) a system of internal controls; (2) independent testing for compliance; (3) the designation of an individual, or individuals, to coordinate and monitor day-to-day compliance; and (4) training of appropriate personnel.[99]

What good do these documentation requirements do? Perhaps the existence of these documentation requirements deters money laundering if criminals fear that there will be a paper trail of their transactions, and the "structuring" crime under the Act attempts to deter efforts to circumvent those reporting requirements.[100] But what must be done to review those millions of reports of transactions is unclear. Banks and their regulators certainly cannot review all the

95. 31 U.S.C. § 5313 (2018); 31 C.F.R. § 103.22(b) (2010).

96. 12 C.F.R. § 21.11(c)(2).

97. 2011 FIN. CRIMES ENF'T NETWORK ANN. REP. 7, https://www.fincen.gov/sites/default/files/shared/annual_report_fy2011.pdf [https://perma.cc/J4GX-VE3W]; *see also* Michael J. Deblis III, *Money Laundering: Is the Anti-Structuring Statute Netting the Small Fry with the Big Fish?*, CRIM. JUST., Summer 2014, at 19 ("[T]oday, the volume of reports filed, especially CTRs, is simply too great, and large cash transactions too common . . . to support the façade of the BSA.").

98. *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, §§ 311, 312, 314, 319, 325 (2001); 31 U.S.C. § 5318(h) (2018), 31 C.F.R. § 103.l8(a)(2) (2010); *see also* 12 C.F.R. §21.11, 21.21 (2011).

99. 31 U.S.C. § 5318(h)(1) (2018); 31 C.F.R. § 103.120 (2010). The OCC's enforcement guidelines were last updated in 2007. *See* Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements (July 19, 2007), https://www.occ.gov/news-issuances/news-releases/2007/pub-other-state-2007-76.pdf [https://perma.cc/64Y7-2DRK].

100. 31 U.S.C. §§ 5322(a), 5324(a).

vast amount of information collected and disclosed under the Act each year. Regulators have issued guidance on how to focus on the highest risk transactions, including with foreign banks.[101] But the U.S. Senate has held hearings where Senators have complained that OCC enforcement had long been lacking, and that AML compliance was seen as a matter of consumer compliance and not the soundness of a bank.[102]

In response, enforcers have increasingly used the big stick of criminal prosecutions, and now more often bring criminal cases when it is revealed after-the-fact that banks' AML programs ignored large numbers of SARs. For example, the prosecution agreement with Wachovia described how the bank had tuned their filtering and search functions to provide less than 100 alerts per month due to a lack of adequate personnel to review more alerts.[103] Further, those alerts did not provide information that permitted ready examination of their suspicious elements.[104] Prosecution agreements with major banks have in recent years required that the banks adopt a "customer risk-rating methodology" in order to better sift through all of the reports generated.[105] Using civil and criminal enforcement to improve compliance at financial institutions may be a good thing if it promotes the use of tools that can better comply with the AML requirements of the Bank Secrecy Act and related statutes and regulations. However, it is not clear that prosecutors or regulators are evaluating what types of risk-rating methods can best sift through the millions of transaction reports and suspicious activity reports, and carefully evaluate them to identify the truly problematic transactions.

Using random sampling to assess the quality of automatic methods, and human judgment in reviewing flagged transactions, would make sense in an area with high volumes of reports. Regulators and prosecutors are in a position to require careful auditing of compliance; after all, banks can lose their charters if convicted of certain crimes, including money laundering crimes.[106] But again, the watchdogs appear unwilling, or unable, to provide direction that encourages evidence-based compliance.

---

101. Financial Crimes Enforcement Network; Anti-Money Laundering Programs; Special Due Diligence Programs for Certain Foreign Accounts, 67 Fed. Reg. 48348, 48350 (July 23, 2002) (codified at 31 C.F.R. §§ 103.181–.183).

102. STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, COMM. ON HOMELAND SEC. & GOV'TAL AFFS., 112th CONG., REP. ON U.S. VULNERABILITIES TO MONEY LAUNDERING, DRUGS, AND TERRORIST FINANCING: HSBC CASE HISTORY 246, 318–21 (Comm. Print 2012) ("The OCC's peculiar treatment of AML concerns as a consumer compliance issue has multiple negative consequences . . . ."); *see also Keeping Foreign Corruption out of the United States: Four Case Histories: Hearing Before the S. Permanent Subcomm. on Investigations of the Comm. on Homeland Security & Governmental Affairs*, 111th Cong. (2010); *Tax Haven Banks & U.S. Tax Compliance: Hearing Before the S. Permanent Subcomm. on Investigations of the Comm. on Homeland Security & Governmental Affairs*, 110th Cong. (2008).

103. Wachovia Bank, N.A, FINCen No. 2010-1, 2010 FINCEN LEXIS 6, at *4 (Mar. 10, 2010).

104. *Id.*

105. *See, e.g.*, Deferred Prosecution Agreement at 6, United States v. HSBC Bank USA, N.A., No. 12-cr-00763 (E.D.N.Y. July 1, 2013), 2012 WL 6120512.

106. 12 U.S.C. § 93(d).

4. Worker Protection Laws

Some of the earliest scholarly concern that organizations might use internal compliance programs to curry favor with incumbents, stockholders, regulators, judges, and juries, rather than to drive substantive change within an organization, arose with respect to laws designed to protect workers from discrimination, unsafe working conditions, and wage theft. In 1992, for instance, the sociologist Lauren Edelman examined the measures companies were putting in place to address discrimination following passage of Title VII of the Civil Rights Act of 1964 (Title VII),[107] and sounded a cautionary note:

> When organizations claim that, by creating [equal opportunity and affirmative action] structures, they have eliminated discriminatory practices, they force courts, lawmakers, and society to struggle with the question of what constitutes compliance. Courts, for the most part, only legitimate or delegitimate forms of compliance that organizations devise. But it is important to keep in mind that most organizations' constructions of compliance are never examined in court. Thus organizations' collective response to law becomes the de facto construction of compliance; it is shaped only at the margins by formal legal institutions.[108]

But Edelman was agnostic as to effects of this turn toward internal compliance: "it remains uncertain at this point whether these structures act as a stepping stone toward the achievement of [equal opportunity and affirmative action] ideals or whether they exist as mere window dressing."[109] Writing ten years later, Professor Kim Krawiec argued that the evidence pointed toward a negative conclusion: "a growing body of evidence indicates that internal compliance structures do not deter prohibited conduct within firms and may largely serve a window-dressing function that provides both market legitimacy and reduced legal liability."[110]

Although there is little evidence that corporations adopted anti-discrimination policies (or other policies nominally directed at protecting workers) with the goal of maintaining and hiding exploitive policies under a mask of cosmetic compliance, the evidence continues to support Professor Krawiec's negative conclusion about the effects of internal compliance programs aimed at protecting workers and promoting diversity.

In-house programs, usually put in place at considerable cost and with the help of outside self-styled expert consultants, often lack any basis in empirical research and often fail to produce any positive change within an organization. For example, Elizabeth Paluck and Donald Green examined a wide variety of anti-discrimination measures that companies are advised to adopt by diversity consultants and concluded that "[w]e currently do not know whether a wide range of programs and policies tend to work on average, and we are quite far from having an empirically grounded understanding of the conditions under

107. 42 U.S.C. 2000e *et seq.*

108. Lauren B. Edelman, *Legal Ambiguity and Symbolic Structures: Organizational Mediation of Civil Rights Law*, 97 AM. J. SOCIO. 1531, 1568 (1992).

109. *Id.*

110. Krawiec, *supra* note 31, at 487.

which these programs work best."[111] Further, Alexandra Kalev, Frank Dobbin and Erin Kelly surveyed corporations about in-house measures aimed at ending workplace inequality and evaluated the effects of these measures using data submitted to the federal government about the representation of women and minorities within in these corporations.[112] They found modest positive effects for some kinds of measures, but many failed to show any effect or were associated with negative effects.[113] In a separate study, Kalev and Dobbin found, in contrast, that compliance reviews by the Office of Federal Contract Compliance Programs (OFCCP)—a process that seeks to alter personnel policies and practices that cause discrimination—were effective at increasing the representation of minorities within companies serving as government contractors.[114]

Aside from OFCCP compliance reviews, the courts, regulators, and private bar have done little to move companies toward empirically-validated programs that promote diversity, prevent discrimination, and prevent exploitation of workers.[115] In a trio of rulings in 1998 in suits alleging workplace discrimination under Title VII, the Supreme Court did recognize an affirmative defense for employers who can show that they took reasonable steps to prevent and correct sexual harassment.[116] But the Court offered little guidance on how to evaluate an internal program, leaving it to lower courts and the parties to litigate this issue case by case. Subsequent studies find little evidence that companies responded to these decisions by instituting effective anti-harassment policies and practices.[117]

---

111. Elizabeth Levy Paluck & Donald P. Green, *Prejudice Reduction: What Works? A Review and Assessment of Research and Practice*, 60 ANN. REV. PSYCH. 339, 357–58 (2009).

112. Alexandra Kalev, Frank Dobbin & Erin Kelly, *Best Practices or Best Guesses? Assessing the Efficacy of Corporate Affirmative Action and Diversity Policies*, 71 AM. SOCIO. REV. 589, 610–12 (2006).

113. *Id.*

114. *See* Alexandra Kalev & Frank Dobbin, *Enforcement of Civil Rights Law in Private Workplaces: The Effects of Compliance Reviews and Lawsuits Over Time*, 31 LAW & SOC. INQUIRY 855, 891 (2006) (explaining that the OFCCP has power to debar companies as government contractors for non-compliance with federal law, including federal affirmative action regulations).

115. *But cf. id.* (highlighting that even OFCCP compliance reviews were less effective in the 1980s than the 1970s).

116. *See* Kolstad v. Am. Dental Ass'n, 527 U.S. 526, 544–45 (1999) (recognizing "good faith efforts at Title VII compliance" as a defense to punitive damages); Faragher v. City of Boca Raton, 524 U.S. 775, 806–07 (1998) (recognizing an affirmative defense to hostile environment claims); Burlington Indus. v. Ellerth, 524 U.S. 742, 764–65 (1998) (holding that in a case absent tangible employment action "a defending employer may raise an affirmative defense to liability or damages, subject to proof by a preponderance of the evidence . . . [t]he defense comprises two necessary elements: (a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior, and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise").

117. *See, e.g.*, Joanna L. Grossman, *The Culture of Compliance: The Final Triumph of Form over Substance in Sexual Harassment Law*, 26 HARV. WOMEN'S L.J. 3, 4 (2003) (noting that updated anti-harassment procedures and programs were created without examining likelihood of harassment prevention and adequate redress); Melissa Hart, *The Possibility of Avoiding Discrimination: Considering Compliance and Liability*, 39 CONN. L. REV. 1623, 1623 (2007) (introducing the issue of workplace discrimination programs failing to improve experiences of women and minorities); John H. Marks, *Smoke, Mirrors, and the Disappearance of "Vicarious" Liability: The Emergence of a Dubious Summary-Judgment Safe Harbor for Employers Whose Supervisory Personnel Commit Hostile Environment*

As one commentator put it, "[t]he problem is that the lower federal courts have interpreted the elements of the affirmative defense so as to reward employers for engaging in behaviors that have little effect on the incidence of workplace harassment."[118]

Regardless of whether employers assert this affirmative defense, the measures a company has in place to detect and prevent discrimination will often be attacked by plaintiffs, usually through an expert witness who opines that conditions in the workplace fostered discrimination.[119] Unfortunately, these experts rarely assess the effects of internal compliance measures using proper empirical studies. Instead, they commonly base their opinions on speculative connections between general research and the individual company at hand.[120] Valid empirical studies can be conducted by experts even in the context of litigation, as often happens with respect to statistical analyses of employment data in discrimination cases.[121] But aside from statistical studies, only rarely do the plaintiffs' experts attempt to assess the effectiveness of internal policies and procedures aimed at protecting workers using valid empirical methods.

Once litigation has begun, companies will examine personnel data for statistically significant differences in pay or representation across demographic groups and occasionally conduct an internal study designed to assess the effects of their anti-discrimination policies because such inquiries can be covered by the work-product doctrine. But companies resist performing internal studies to assess the effects of their anti-discrimination policies without the protection of a privilege for fear of creating evidence that will be used against them in litigation. Such studies would likely have the benefit of improving compliance and preventing litigation in the first instance, but absent a good prediction of what

Workplace Harassment, 38 HOUS. L. REV. 1401, 1435–36 (2002) (describing the creation of a safe harbor which erases vicarious liability for employers who implement anti-harassment policies that include a complaint mechanism); David Sherwyn, Michael Heise & Zev J. Eigen, *Don't Train Your Employees and Cancel Your "1-800" Harassment Hotline: An Empirical Examination and Correction of the Flaws in the Affirmative Defense to Sexual Harassment Charges*, 69 FORDHAM L. REV. 1265, 1298–1301 (2001) (explaining that a short statute of limitations on reports of sexual harassment can negatively affect workplace culture and deny reasonable remedies to injured plaintiffs); Susan Sturm, *Second Generation Employment Discrimination: A Structural Approach*, 101 COLUM. L. REV. 458, 462–63, 567 (2001) (discussing the increased utility of a structural approach to combat employment discrimination as opposed to a rule-enforcement and regulatory approach).

118. Anne Lawton, *Operating in an Empirical Vacuum: The* Ellerth *And* Faragher *Affirmative Defense*, 13 COLUM. J. GENDER & L. 197, 198 (2004).

119. *See* John Monahan et al., *Contextual Evidence of Gender Discrimination: The Ascendance of "Social Frameworks,"* 94 VA. L. REV. 1715, 1716–17 (2008) (describing the increasingly important role of experts who provide context to help understand the specific facts of discrimination suits).

120. *See id.* at 1749 ("If testimony about a specific case is to be offered by an expert, that testimony should be based on valid 'social fact' research that involves the parties before the court, rather than on subjective, unscientific extrapolation from general research conducted outside the case.").

121. *See* Gregory Mitchell, Laurens Walker & John Monahan, *Beyond Context: Social Facts as Case-Specific Evidence*, 60 EMORY L.J. 1109, 1115–16 (2011) (explaining that employment discrimination cases commonly use statistical evidence to prove that being a member of a protected class is predictive of employment outcomes).

the costs and benefits will be, companies remain leery of self-critical audits and data analysis outside of the litigation context.

Nor do courts, government regulators or the plaintiffs' bar, when in a position to compel validated compliance programs through entry of a consent decree or approval of a class action settlement, insist that companies build validation testing into their compliance programs. Indeed, a sample of the consent decrees entered into by companies with the Equal Employment Opportunity Commission (EEOC) between 1999 and 2009 revealed that many of these agreements put in place measures similar to those criticized by the experts retained by the EEOC or plaintiffs in litigation.[122] They also fail to follow evidence-based recommendations on how to prevent discrimination, much less require that companies engage in periodic testing to determine what effects the measures are having. As we saw with respect to enforcement under the FCPA and BSA, those with power to compel validation of internal compliance measures rarely exercise that power.

III
COMPLIANCE AMONG THE FORTUNE 100

Although prosecutors and regulators do not insist on empirical validation of compliance, it is possible that firms nevertheless engage in such assessments to make cost-benefit-driven decisions about compliance investments. In our experience discussing these issues with chiefs of compliance, in-house counsel, and lawyers who focus their practices on compliance issues, we have learned that such internal validation does not typically occur. The validation efforts that do occur typically involve examining incident levels over time and surveying employees about their knowledge and attitudes on compliance-related topics; both of these approaches can provide only limited information about the validity of a compliance program.

However, our anecdote-based understanding may be inaccurate or applicable to only a limited set of companies. Presently, little is systematically known about the degree to which companies invest in compliance or what form that compliance takes.[123] Some industry surveys have occurred, but it is not clear that such surveys provide representative information about compliance within even the industries of focus, much less regarding for-profit corporations generally.[124]

122. The assertions in this paragraph derive from a review of cases supplied by the EEOC, in which it entered into a consent decree. A list of these cases are on file with *Law and Contemporary Problems*. *See also* LAUREN B. EDELMAN, WORKING LAW: COURTS, CORPORATIONS, AND SYMBOLIC CIVIL RIGHTS 168–213 (2016) (discussing how courts and the EEOC have deferred to organizations with respect to proper measures for preventing discrimination); *Consent Decrees*, DIGIT. COMMONS AT CORNELL UNIV. INDUS. LAB. REL. SCH. (2019), https://digitalcommons.ilr.cornell.edu/condec/index.html [https://perma.cc/BK3L-UVSV] (maintaining a collection of EEOC consent decrees).

123. Sean J. Griffith, *Corporate Governance in an Era of Compliance*, 57 WM. & MARY L. REV. 2075, 2100 (2016).

124. John Armour, Brandon Garrett, Jeffrey Gordon & Geeyoung Min, *Board Compliance*, 97 MINN. L. REV. 1191, 1207 (2020).

Nor are companies required to disclose information about their compliance expenditures. The SEC has required public companies to disclose information about audit, compensation, and nomination committees, which led to a practice of similarly disclosing information, such as charters, for other committees, including board-level compliance committees.[125] There is evidence, however, that the vast majority of public corporate boards do not create board-level compliance committees.[126]

To shed some additional light on this question, we examined what the Fortune 100 companies say about their compliance programs in publicly available sources.[127] Of those companies, eighty-six described their compliance programs in some detail, while fourteen did not go into any detail; every company at least stated which group within the firm was responsible for compliance.[128] Seventy-six companies described efforts to train and educate officers and employees regarding compliance obligations.[129] Many of these companies made compliance policies available online, sometimes with distinct policies applicable to different areas of their business; eighty-one make a code of ethics or code of conduct available online.[130] Many firms—seventy-seven of them—described to whom anonymous reports of non-compliance can be made, and of this subset, fifty-nine reported that an executive-level officer was responsible for compliance, with all but one reporting to the Board of Directors.[131]

Consistent with our personal observations, far less is disclosed concerning auditing of the compliance measures. Ninety companies did describe efforts to audit or assess compliance, but for almost all of those companies, it simply involved making clear that anyone can report noncompliance and noting that an audit committee can further investigate instances of noncompliance. A handful of companies state that they conduct risk management efforts to assess

125. 17 C.F.R. § 299.407 (2006); Armour et al., *supra* note 124, at 1221–25 (discussing case studies of board-level compliance committees).

126. Armour et al., *supra* note 124, at 1225.

127. FORTUNE 500 LIST OF COMPANIES 2020, https://fortune.com/fortune500/2019/search/ [https://perma.cc/M382-TUZD]. We studied the first 100 companies listed. Two research assistants examined each company's public websites to determine what information relating to compliance was publicly disclosed using a structured review examining what details are disclosed, including information about training, compliance audits, whistleblower reporting avenues and protections, resources devoted to compliance, and authority over compliance programs. All data are on file with authors.

128. *Id.*

129. *Id.*

130. *Id.*

131. *Id.*

compliance,[132] while others rely on employee surveys to gauge the effectiveness of training.[133]

This evidence suggests that the largest companies do not publicize efforts to assess compliance rigorously, but that does not mean such efforts are not occurring. However, if the Fortune 100 companies are measuring the effectiveness of their compliance programs, they are not sharing it. It is also possible that what we see is what we get: active educational efforts focused on employee training and assessments of that training using employee surveys and reactive compliance efforts relying on whistleblower reporting and investigation of those reports. The public record reveals few active efforts to detect and remedy weaknesses within internal compliance systems.

IV
INCENTIVIZING VALIDATED COMPLIANCE

To better understand why companies may be reluctant to validate their compliance programs or put in place strong programs, we need to understand the costs and benefits of adopting a strong compliance program. A company's calculus about whether to put in place a strong compliance program will involve direct and indirect costs and benefits. The direct costs and benefits arise when the law or regulators have either mandated compliance (as with some measures required under the BSA) or purport to reward compliance (as with the downward departure recommended under the Organizational Guidelines). High penalties directly tied to ineffective compliance or big rewards directly tied to effective compliance may be sufficient to motivate companies to install strong compliance programs. However, if those enforcing the laws mandating or rewarding compliance cannot or will not distinguish between effective and ineffective compliance programs, then rational companies will look to indirect costs and benefits to determine what resources to devote to compliance. Indirect costs and benefits will depend on the relative costs of strong compliance versus liability for illegal behavior that may occur absent strong compliance, as well as the likelihood of detection and prevention of illegal behavior with and without an effective compliance program in place. This includes the risk of creating incriminating evidence that may be available to whistleblowers and government regulators.

132. *E.g.*, *How We Manage Enterprise Risk*, *Ethics & Compliance*, RAYTHEON TECHS., https://www.rtx.com/our-company/ethics-and-compliance [https://perma.cc/6NYN-VCMA] (listing five key areas of compliance risk: antitrust, corruption, data privacy, government contracts, and international trade); *Compliance Process Reviews*, *Monitoring & Auditing*, HCA HEALTHCARE, https://hcahealthcare.com/ethics-compliance/monitoring-and-auditing.dot [https://perma.cc/Q846-S55D] (detailing the procedures for assessing whether facilities follow ethical standards).

133. *E.g.*, *Business Conduct Compliance Training*, LOCKHEED MARTIN, https://www.lockheedmartin.com/en-us/who-we-are/ethics/business-conduct-compliance-training.html [https://perma.cc/2ULE-RSK9] (sending surveys to employees to gauge the effectiveness of Lockheed's business conduct compliance training).

A complicating factor for companies calculating the direct costs associated with compliance programs is the fact that compliance with one legal regulator's mandates or commands is not likely to provide immunity from liability to other regulators or private parties that seek to impose liability on the company. Even behavior that may appear to be the exclusive domain of federal regulation, such as dealings with officials in foreign countries under the FCPA, may be subject to parallel litigation where the behavior may affect stock prices or tax obligations.[134] The threat of parallel litigation frustrates the ability of any one regulatory actor to incentivize and reward compliance.

Nonetheless, a single law or powerful regulator could set penalties or rewards at such high levels that the single mandate or promise of reward would be sufficient to motivate investments in strong compliance programs. However, as discussed in Part II, the laws that directly mandate or reward compliance provide little guidance on what is required and do not mandate proof of effectiveness, and the courts, regulators, and prosecutors applying these laws do not consistently reward strong compliance or consistently punish weak compliance.

Accordingly, companies are more likely to make decisions about compliance investments based on indirect costs and benefits. A simple deterrence model provides a useful starting place for how companies are likely to address this question: as Professors Arlen and Kraakman have shown, under this model, companies should invest in compliance when the cost of doing so reduces the expected sanction from government enforcers or others, given the likelihood of detection of the conduct, to an amount below the compliance costs. If the sanction is low, or the likelihood of detection is low, one would expect little investment in compliance. But as Arlen and Kraakman note, this simple model is complicated by a potentially perverse fact: the risk of sanction increases as investments in compliance increase, offsetting gains from the compliance.[135] Rational companies may fear investing in compliance precisely because it will uncover violations that would otherwise not be discovered, leading to greater net sanctions. For this reason, Arlen and Kraakman advocate a "composite" regime that clearly rewards compliance and self-reporting with reduced sanctions.[136]

Social welfare should increase under this regime if regulators reward effective but not cosmetic compliance, for the former should reduce the overall level of socially undesirable behavior while the latter may conceal, and even perpetuate, such behavior. Professor Arlen has recommended that prosecutors set their fines to incentivize compliance and reward self-reporting of violations, while giving civil regulators sole authority to impose and assess structural reforms.[137]

134. GARRETT, *supra* note 46, at 137–40 (describing parallel civil litigation).

135. Arlen & Kraakman, *supra* note 36, at 706–11 (discussing the impact of policing measures on likelihood of sanctions).

136. *Id.* at 687.

137. *See generally* Jennifer Arlen, *Removing Prosecutors from the Boardroom*, *in* ANTHONY BARKOW & RACHEL BARKOW, PROSECUTORS IN THE BOARDROOM: USING CRIMINAL LAW TO REGULATE CORPORATE CONDUCT 79 (Anthony S. Barkow & Rachel E. Barkow eds., 2011).

Although the legal apparatus for this composite regime exists, as discussed in Part II, it does not appear that we have this regime in practice. In the following Subparts, we discuss existing proposals aimed at putting in place the sort of regime that Professors Jennifer Arlen and Reinier Kraakman proposed, problems with these proposals, and how we might move toward a real composite regime that rewards effective compliance programs.

A. Existing Proposals

In this Subpart, we discuss two prominent proposals aimed at encouraging compliance that have been advanced by the business community and scholars, in particular, a compliance defense and a privilege for compliance-related evidence. We argue that neither is sufficient to cause companies to engage in validation of their compliance programs.

1. A Compliance Defense

Many scholars have noted that failure to give adequate credit for compliance creates perverse incentives for companies.[138] Some have proposed a compliance defense, with most of the scholarship focusing on criminal law,[139] and arguing more states should adopt the Model Penal Code, which recognizes a compliance defense.[140] The Second Circuit Court of Appeals rejected an argument that federal corporate criminal liability should be limited in that way, citing longstanding federal law permitting corporate criminal liability for actions of employees acting in the scope of their employment.[141] Professor Peter Henning argues that companies should "be careful what they wish for": when a compliance defense is raised, prosecutors could dig deep into the effectiveness of the company's policies.[142] Absent such digging by prosecutors, however, it will be difficult to determine whether the company's compliance program had teeth or was merely window dressing. Compliance demands will vary by size of the

138. Arlen & Kraakman, *supra* note 36.

139. *See*, *e.g.*, Mike Koehler, *Revisiting a Foreign Corrupt Practices Act Compliance Defense*, 2012 WIS. L. REV. 609, 658–59 (2012) (arguing for an FCPA compliance defense to incentivize self-reporting violations); Charles J. Walsh & Alissa Pyrich, *Corporate Compliance Programs as a Defense to Criminal Liability: Can a Corporation Save its Soul?*, 47 RUTGERS L. REV. 605, 607–08 (1995) (noting that "corporate compliance programs only rarely deflect criminal liability"). Some scholars have instead argued that corporate criminal liability should be limited to cases where upper management encouraged agents to commit crimes. William S. Laufer, *Corporate Bodies and Guilty Minds*, 43 EMORY L.J. 647, 677 (1994). One scholar proposed a compliance defense to punitive damages in civil tort actions. Charles M. Foster, Jr., et al., *Compliance Programs: An Alternative to Punitive Damages for Corporate Defendants*, 49 S.C. L. REV. 247, 263 (1998).

140. MODEL PENAL CODE § 2.07(5) (AM. LAW INST. 1962).

141. United States. v. Ionia Mgmt. S.A., 555 F.3d 303, 310 (2d Cir. 2009) (per curiam) (citing United States v. Twentieth Century Fox Film Corp., 882 F.2d 656, 660 (2d Cir. 1946)).

142. Peter J. Henning, *Be Careful What You Wish For: Thoughts on a Compliance Defense Under the Foreign Corrupt Practices Act,* 73 OHIO ST. L.J. 883, 922–24 (2012) (discussing how prosecutors would respond to a corporate compliance defense); *see also* Howard Sklar, *Against An FCPA Compliance Defense*, FORBES (Oct. 18, 2011), https://www.forbes.com/sites/howardsklar/ 2011/10/18/against-an-fca-compliance-defense/#5b59527f34b5 [https://perma.cc/FPW9-C4JF] (arguing a compliance defense would lead to unintended consequences).

workforce and nature of the compliance risks: what works for one company may not work for another.[143] Furthermore, few cases go to a trial, making the benefits of such a defense in incentivizing compliance equivocal. Thus, while legal recognition of a compliance defense may encourage some companies to invest in effective compliance programs, the calculus is much more complicated than it may at first appear.

Nevertheless, an existing compliance defense already exists informally in that prosecutors and a range of regulators examine compliance when deciding whether to offer leniency during settlement negotiations with corporations, and this practice has encouraged a growing compliance industry. As detailed above, however, this practice and the resulting compliance programs do not focus on effective compliance. Moreover, while companies know that prosecutors and regulators often value compliance, they also know that empirical evidence of effectiveness will often not be demanded and that the overseers will look at other factors, such as seriousness of violations, cooperation, ability to pay fines, and a host of others to make charging and plea decisions and sentencing recommendations.

Uncertainty about the availability of a broad compliance defense under the law or a compliance discount in practice will lead many companies to question how many resources to devote to compliance. In order to incentivize effective compliance, the law and overseers need to require proof that compliance measures are being rigorously evaluated before the compliance defense or a compliance discount is available, and the circumstances where the defense and discount will apply need to be clear and predictable. Clarity in application, combined with a requirement of rigor, will allow companies truly committed to effective compliance to benefit from their investments—leading those companies to welcome rather than fear outside investigations into their compliance records—and will discourage companies from investing in meaningless compliance programs that today may be rewarded by regulators who fail to focus on rigor.

2. A Compliance Privilege

An alternative proposal to encourage compliance is to privilege compliance information whether generated under the direction of lawyers or not, thereby extending protection for compliance information beyond that currently available under the work-product and attorney-client privileges. Traditionally, privileges are created where an important societal goal will be served by ensuring confidentiality for the production of information or the communication of information.[144] As shown by the increasing emphasis on internal compliance,

143. Shaun Cassin, *The Best Offense is a Good Defense: How the Adoption of an FCPA Compliance Defense Could Decrease Foreign Bribery*, 36 HOUS. J. INT'L. L. 19, 45 (2014) ("Compliance programs should be tailored to the specific needs of each company that implements one.").

144. *See* EDWARD J. IMWINKELRIED, THE NEW WIGMORE: EVIDENTIARY PRIVILEGES § 3.2.1 (3d. ed. 2016) (discussing competing instrumental rationales for evidentiary privileges).

lawmakers and regulators see considerable value in having organizations self-regulate, and every indication is that organizations are in fact investing in compliance programs, as shown by our discussion of the Fortune 100. What is missing is evidence that organizations are investing in *effective* compliance. Would a compliance privilege provide a way out of the compliance trap?

Advocates of a compliance privilege argue that, because of the perverse effects that may come from effective compliance, namely, that the risks of detection and sanctions increase when an organization vigorously polices itself, a privilege is necessary to remove this perverse effect. The idea is that once companies no longer fear that vigorous self-policing will increase litigation risks, they will engage in more compliance efforts and undertake self-critical analyses of those efforts to make them more effective at preventing misconduct that may be costly to the organization. The fear of opponents of compliance privilege is that the privilege will be used to conceal otherwise discoverable information about an ineffective compliance program and shoddy efforts to investigate and prevent wrongdoing by organizational insiders.

Aside from the political opposition by skeptics of internal compliance, many practical problems plague the privilege proposal. Most notably, absent parallel privileges under state and federal law, as well as international law for global players, a compliance privilege is unlikely to disabuse companies of their fear that information from their audits of internal compliance programs will see the light of day and be used against them. In addition, the privilege would need to address what counts as compliance-related information for purposes of the privilege and with whom the information may be shared without losing the privilege. To the extent a broad answer is given to each question, the chance that companies will abuse the privilege increases, but a broad approach is needed to encourage companies to engage in organization-wide assessments of compliance programs without the hurdles imposed when only the work-product and attorney-client privileges provide protection.

The limits placed on what can be done and who can participate in compliance review by having to operate under only the attorney-client and work-product privileges are substantial. For instance, one commentator, while recommending the creation of a "culture of compliance," strongly counsels that "the matter should be referred to the corporation's legal counsel for review, investigation, and legal analysis,"[145] and one recommended compliance questionnaire reads:

> Do not at this time prepare any written notes, tape recordings, memoranda, or any other tangible material relating to this questionnaire. Also, do not at this time provide anyone else, except your attorney, with any information, either oral or written, relating to this questionnaire. (DON'T pass this around the office for comment.)[146]

Such guidance hampers communication and self-critical scrutiny, even if it does help maintain privilege. Moreover, to fulfill the promise of internal compliance,

145. H. Lowell Brown, *The Corporate Director's Compliance Oversight Responsibility in the Post* Caremark *Era*, 26 DEL. J. CORP. L. 1, 141 (2001).

146. ROBERT B. HUGHES, LEGAL COMPLIANCE CHECKUPS: BUSINESS CLIENTS § 2:1 (2020).

companies need to engage in compliance audits before litigation is on the horizon—indeed, the goal is to head off behavior that might lead to criminal or civil liability—but a business motivation or a desire to reduce litigation risks generally may take the audit outside the protection of the work-product doctrine.[147]

Some state statutes create privileges that extend beyond the attorney-client and work product privileges and can be used to protect audits of internal systems under some conditions. For example, a Colorado statute privileges environmental audits on the theory "that limited expansion of the protection against disclosure will encourage such voluntary compliance and improve environmental quality and that the voluntary provisions of this act will not inhibit the exercise of the regulatory authority by those entrusted with protecting our environment."[148] Perhaps most common is a privilege for discussions of hospital peer review committees, the idea being that such a privilege will improve patient safety by encouraging candid review of the causes of a bad medical outcome.[149] Some states even privilege self-critical analysis generally, but most states have declined to adopt such a privilege.[150] Even when a state has adopted a privilege that might cover compliance audits, the privilege will not apply in federal court where a federal law is at issue,[151] and federal agencies may not honor the state law privilege (for example, the EPA does not recognize the environmental audit privilege).[152] Likewise, although a few federal courts have recognized a qualified self-evaluative privilege for reports mandated by the government and for an institution's self-critical analysis,[153] state and federal courts are not bound to apply the privilege with respect to state law issues.[154]

The idea behind a compliance privilege is sound because it addresses a key cause of the compliance trap: a fear that internal reviews of compliance programs will be used against the company. But the privilege proposal raises political and

147. S. Bell Tel. & Tel. Co. v. Deason, 632 So. 2d 1377, 1384 (Fla. 1994).

148. COLO. REV. STAT. § 13-25-126.5(1) (2016); *see also* CAROL DECK, CORPORATE COMPLIANCE SERIES: ENVIRONMENTAL § 2:7 (2020) (identifying other states with similar environmental privileges).

149. *See generally* IMWINKELRIED, *supra* note 144 at § 7.8.2 (2014) (discussing privilege for medical peer review).

150. *See, e.g.*, WIS. STAT. § 146.38 (2019) (articulating a broad confidentiality for self-evaluations in health care); Roman Catholic Diocese of Jackson v. Morrison, 905 So. 2d 1213, 1245 (Miss. 2005) (declining to recognize self-critical analysis privilege).

151. FED. R. EVID. 501.

152. Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations, 60 Fed. Reg. 66,706, 66,707 (Env't Prot. Agency, Dec. 22, 1995).

153. *Compare*, Bredice v. Doctors Hosp., Inc., 50 F.R.D. 249, 251 (D.D.C. 1970) (recognizing a self-critical analysis privilege in context of hospital peer review), *with* James F. Flanagan, *Rejecting a General Privilege for Self-Critical Analyses*, 51 GEO. WASH. L. REV. 551, 574–76 (1983), *and* Ronald G. Blum & Andrew J. Turro, *The Self-Evaluative Privilege in the Second Circuit: Dead or Alive?*, 75 N.Y. ST. BAR ASS'N J., June 2003, at 44, 45 (listing federal court decisions rejecting the privilege). *See generally* Clyde C. Kahrl, *The Attorney-Client Privilege, the Self-Evaluation Privilege, and Diversified Industries, Inc. v. Meredith*, 40 OHIO ST. L. J. 699 (1979) (describing different approaches federal courts take in applying evidentiary privileges).

154. FED. R. EVID. 501.

practical problems that make it of limited use in really solving the compliance trap. We propose a related, but different approach that seeks to address the practical and political problems associated with prior privilege proposals.

B. An Alternative Approach: Mandated Confidential Reporting of Validation Efforts and Results

To many public and private watchdogs, giving companies a privilege for compliance information will do little more than allow companies to hide misbehavior and their failures to prevent it. As one court noted when rejecting a self-critical privilege in an employment case, "Carried to its logical extreme, such a privilege would foreclose discovery of material which might be most strongly probative of discriminatory intent."[155] And even if the privilege is applied uniformly across courts and administrative proceedings, the problem remains that the organization may lack the willpower or know-how to engage in proactive efforts to audit compliance systems whether the privilege exists or not. What is needed, in short, is a legal mandate that organizations regularly test their compliance systems for effectiveness. But to incentivize companies to put in place strong compliance programs and audit those programs rigorously, the mandated reports should not increase their litigation exposure. To do this, the mandatory reports cannot become litigation fodder.

Following the model of the Employer Information Form (known informally as the EEO-1 form) that companies must submit under federal employment law, we propose that companies be required to report their efforts to validate compliance programs, and the results of that testing, to the federal government.[156] Failure to file the form would subject the company to fines or other penalties, such as debarment or delisting, as would the making of willfully false statements in the reports, as is the case with EEO-1 forms.[157] No requirements would be set on what compliance measures must be in place, but the measures put in place must be evaluated using a disclosed methodology, including a disclosure of the outcome measures used and a detailed description of the data on which the report is based. The information would not report details of any individual incidents of misbehavior detected—that is, summary descriptive statistics would be reported—and would remain confidential under federal law, as is the case with EEO-1 reporting.

Regulators would not be able to use the information provided in enforcement efforts, contrary to the case with EEO-1 information which can be used in government enforcement efforts.[158] Additionally, the compliance data provided and evidence related to reviews undertaken to satisfy the reporting requirement would not be admissible against the company in any proceeding by a government

155. Webb v. Westinghouse Elec. Corp., 81 F.R.D. 431, 433–34 (E.D. Pa. 1978).

156. *EEO-1 Survey*, U.S. EQUAL EMPLOYMENT OPPORTUNITY COMM'N, https://www.eeoc.gov/employers/eeo-1-survey [https://perma.cc/C29S-774U].

157. *Webb*, 81 F.R.D. at 433–34.

158. *Id.*

agency or other party except with respect to an action enforcing the reporting requirement or seeking to impose a penalty for failure to file. Organizations would be free to waive confidentiality and introduce the data and supporting evidence as part of a defense or to use the information in connection with plea negotiations or a sentencing report. Furthermore, organizations would be free to share compliance information with other companies or even publicize their compliance disclosures if they sought to compete with other companies regarding the rigor of their compliance systems and audits of those systems. We propose that the place to start for such reporting is with public companies that are subject to SEC oversight, given the federal government's legitimate interest in regulating publicly-traded companies and the attendant broad powers available to the SEC to compel disclosure of information related to internal controls.[159]

The reporting requirement would not mandate use of any particular compliance measures, leaving that to the company to determine in light of other laws and the benefits that may come from internal compliance. This alternative approach addresses three of the factors that give rise to the compliance trap: organizational fear that compliance audits create dangerous information, the reluctance of organizational insiders to test their own programs due to the reputational harms that may come from failed interventions, and the failure of courts, prosecutors and regulators to compel companies to validate their compliance programs. However, because it is agnostic on specific measures to put in place and how to evaluate them, this new framework would not address other causes of the compliance trap, namely, the lack of information about what works and the lack of sound testing needed to find out what works. We address these problems in the next Part.

V
FINDING WHAT WORKS

A mandate to engage in compliance validation does not mean that all companies will employ the same measures or means of validation. Depending on risks within particular industries, the needs of particular companies, and applicable laws and regulations, different compliance regimes will be tested with different results. Mandated reporting offers the opportunity to harness new data to examine the effects of different compliance approaches.

A. Compliance Cartels

By ensuring that a large set of regulated entities must validate their compliance programs, the mandate presents the opportunity for coordination among similarly situated companies to leverage knowledge. Members of the compliance cartel agree to share information and, often, to abide by codes of conduct that collectively benefit the group, but which could put individual

159. *See* SEC Form Requirement Rule, 17 C.F.R. § 210 (2003) (listing disclosure requirements for internal financial and audit forms).

companies at a comparative disadvantage absent coordinated group efforts. We have examples of subsets of companies already engaging in such efforts, such as the defense industry in the 1980s combining efforts in wake of military procurement scandals and an effort spearheaded by the Siemens Corporation to bring together companies and government anti-corruption officers to agree on ethics rules when contracting in foreign countries in order to prevent bribery and other forms of corruption.[160]

To prevent defection among members of the cartel, the members agree to tell one another if misconduct is discovered and even blow the whistle with government regulators if the misconduct persists. Siemens has described how, as part of the collective actions regarding corruption it initiated, Siemens promises to tell management of a competing company if it hears about an agent engaging in behavior that violates the code of conduct.[161] In areas where competitors cannot monitor one another easily, however, compliance cartels may serve only as an information-sharing source to learn effective compliance measures more quickly and efficiently.

To learn what works to prevent misconduct, companies need to do more than measure employee understanding of their obligations under the law and code of conduct and investigate an area for misconduct only when a complaint is filed. Companies need to proactively test whether their employees, when given the chance to misbehave, really do. Such testing need not involve comprehensive data collection or expensive analytics, although firms increasingly use such tools, and consultants may market AI approaches to compliance. Rather, experiments, relying on blind performance testing of randomly sampled employees, can quite inexpensively measure whether employees comply in realistic work situations. We have previously argued that all expertise proffered in court should be validated through proficiency testing.[162] Compliance can similarly be tested, through simple in-house experiments.

B. Compliance Testing

Companies test the performance of their employees in a wide range of settings, using job and personality tests to determine whether they have the basic knowledge, skills, and abilities to perform a particular job, using drug and alcohol tests to promote safety and integrity, using proficiency testing to measure accuracy and train, and using in-house phishing tests to monitor information technology security. In some fields, performance testing is standard and required. For clinical laboratories, all employees examining samples for potentially cancerous cells are routinely tested for proficiency pursuant to federal legislation,

160. *Collective Action*, SIEMENS, https://new.siemens.com/global/en/company/sustainability/compliance/collective-action.html [https://perma.cc/NL78-ZBA5] (describing initiatives called "integrity pacts" and "collective actions," following a proposal by Transparency International).

161. GARRETT, *supra* note 46, at 173, 194 (describing "integrity pacts" entered by Siemens).

162. Brandon L. Garrett & Gregory Mitchell, *The Proficiency of Experts*, 166 U. PA. L. REV. 901 (2018).

the Clinical Laboratories Improvement Act.[163] Courtroom interpreters must demonstrate minimal and objective proficiency in order to be hired.[164] We have argued that for forensic laboratories, blind proficiency testing should be more routinely used to assess the accuracy of lab analysts.[165] Currently, accreditation requirements do require annual proficiency testing in a minimal form.[166] Further, as in other areas of performance, an individual person may not perform consistently over time.[167]

Any expertise can be empirically assessed, based on a standard of performance.[168] Compliance is no exception. Employees can be given tasks, resembling those they would ordinarily be given in their work, where the correct answer is known. Such a test is blind. They can be given work that they themselves did some time in the past, which they might not recall, to measure consistency of their performance over time. Compliance tests can assess, for example, whether employees report transactions or results that raise compliance flags. In banking, those might be suspicious transaction reports that require further investigation. In the foreign bribery context, it might involve conducting further due diligence on a vendor.[169] In the environmental context, it might involve a borderline reading from an emissions test, and the need to inquire further. For each, quality or compliance staff can assess whether employees perform appropriately when compliance issues arise in these mock cases.

In domains where the risks associated with certain behaviors are high and consequential, the company may want to employ more aggressive testing, such as examining how employees working in foreign countries respond to a request for a bribe. Alternatively, to test for internal reporting of misconduct, simulated misconduct could be displayed or made known to employees to determine whether the misconduct gets reported. Although such aggressive efforts may

163. Proficiency Testing, Clinical Laboratory Improvement Amendments of 1988 ("CLIA"), 42 C.F.R. § 493(h); *see generally* Garrett & Mitchell, *supra* note 162, at 915–17 (discussing the federal CLIA Act of 1967 and its subsequent amendments).

164. *See Federal Court Interpreter Certification Examination*, U.S. COURTS, http://www.uscourts.gov/services-forms/federal-court-interpreters/federal-court-interpreter-certification-examination [https://perma.cc/4H9N-S6X6] (describing the examinations required to be certified as a federal court interpreter).

165. Garrett & Mitchell, *supra* note 162, at 918–24.

166. *Id.*

167. Daniel Kahneman, Andrew M. Rosenfield, Linnea Gandhi & Tom Blaser, *Noise: How to Overcome the High, Hidden Cost of Inconsistent Decision Making*, HARV. BUS. REV., Oct. 2016, at 38, 40 (finding that professionals are inconsistent decision makers when presented the same data at different times).

168. *See* David J. Weiss & James Shanteau, *Empirical Assessment of Expertise*, 45 HUMAN FACTORS 104 (2003) ("The ideal is to correlate action with a gold standard, an unequivocally valid, universally accepted outcome measure that directly reflects the behaviors under scrutiny.").

169. See, e.g. Joseph E. Murphy, The ISO 37001 anti-corruption compliance program standard: What's good, what's bad, and why it matters (Jan. 14, 2019) (unpublished manuscript), https://ssrn.com/abstract=3315737 [https://perma.cc/JH27-EU7N] (describing ISO requirements to "continually review" anti-corruption compliance but noting unclear and circular definition of "effectiveness" with reference to the company's own "planned results").

cause some employees to feel they are not trusted, given the legal mandate for compliance validation, the organization can attribute the testing to the law rather than a lack of trust. Likewise, organizations can emphasize the risks that come from a lack of compliance, such as breach of information security systems that can lead to calamitous results as with the Equifax breach, to reduce employee concerns or opposition to the testing program. Moreover, for many issues the testing need not involve efforts to detect criminal behavior but rather testing to determine whether existing internal control and educational efforts are effective. Just as the TSA regularly conducts experiments to examine whether different procedures and training are needed to detect dangerous items,[170] companies can use experiments to find areas where new controls and training are needed.

Such blind performance testing is not as expensive as data mining systems offered by vendors. It can be done using random samples of employees or focused testing on units or the areas of greatest concern. If knowledge of such testing becomes widespread within a company, then efforts must be taken to make sure employees cannot discern the testing when it occurs. For instance, imagine submitting fake suspicious financial transactions to measure detection; the main challenge would be ensuring that employees will not be able to distinguish decoys from real transactions. In the context of proficiency testing fingerprint examiners, the Houston Forensic Science Center (which conducts forensic testing for area police enforcement) addressed the problem by making it a game: employees receive a Starbucks card if they correctly guess that a case is a test, while they must pay the lab CEO a dollar if they guess wrong.[171] Before too long, the common reasons why employees suspected that a case was a blind test were identified, and the proficiency testing scheme became widely operational within the lab.[172]

Compliance testing should not just be used to test the performance of individual employees; proficiency testing can also be used to measure system performance. Thus, testing can assess whether compliance programs are working. If employees, after receiving a compliance training or new compliance rules, subsequently pass blind tests, then perhaps that training or those rules are working. If employees fail, then questions arise whether it is a poorly performing employee, or a poorly performing compliance system. Companies can conduct internal experimental studies, rolling out changes to compliance, in part, to assess whether the employees subject to new procedures perform better. Doing so may be cumbersome, but it limits the cost of rolling out an entirely new program before knowing whether it works. Such efforts could involve academics with expertise in research design who could provide internal reports or publish academic work with anonymized data to inform compliance efforts generally.

170. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-633T, AVIATION SECURITY: TSA HAS TAKEN STEPS TO CONDUCT MORE RISK-INFORMED COVERT TESTS AND ADDRESS VULNERABILITIES (2019), https://www.gao.gov/assets/700/699951.pdf [https://perma.cc/9VCH-GXMR].

171. BRANDON L. GARRETT, AUTOPSY OF A CRIME LAB Ch. 9 (forthcoming, U. Cal. Press, 2021).

172. *Id.*

Indeed, the ultimate goal should be to create strong compliance programs that can serve as effective defenses when a company is threatened with litigation and to generate compliance data that can be used to inform enforcers and regulators on compliance efforts that we know work well.

C. Data Mining

Corporations have powerful tools available to analyze internal data and detect violations. Corporations keep far more data concerning employee communications and behavior than ever before. That data can be, and increasingly is, mined for information that might create red flags worthy of investigation. In the FCPA arena, data concerning contracting and payments to third-party vendors can be analyzed for suspicious transactions.[173] Government regulators and investigators themselves increasingly use data-mining techniques. In the area of health care fraud, predictive analytics are used to detect fraudulent billing.[174] For example, using these new systems, regulators uncovered false hospital billing in the WakeMed case in North Carolina when they noticed abnormal patterns in the billing records.[175] More broadly, the FBI advertises that it is promoting "sophisticated data-mining techniques to identify patterns of fraud, systemic weaknesses, and aberrant billing activity."[176] The FBI uses data mining to detect mortgage fraud and in 2009 created a Financial Intelligence Center "to provide tactical analysis of financial intelligence datasets and databases" and uncover securities fraud, money laundering, and other financial fraud.[177] If regulators and investigators are increasingly using such techniques, there will be more pressure, of course, for industry to use similar techniques to detect and prevent violations before they come to the attention of the authorities.

D. Audits

A company, or its auditors and monitors, may conduct unannounced and surprise examinations of a company's business. They may select paperwork or contracts or transactions at random, using a random sampling strategy. Such efforts can similarly be targeted towards risk areas. Blind and random auditing may have a real deterrent effect encouraging compliance, if the program is truly blind and if it is advertised within the organization. Relatedly, in the FCPA area

---

173. Joseph Warin, Michael Diamant & Oleh Vretsona, *How to Use Company Data Efficiently to Detect Fraud and Corruption*, FINANCIER WORLDWIDE MAGAZINE (Aug. 2013), https://www.financierworldwide.com/how-to-use-company-data-efficiently-to-detect-fraud-and-corruption#.X8p66thKiUl [https://perma.cc/B87J-4HGA].

174. U.S. GOV'T ACCOUNTABILITY OFF., GAO-13-104, MEDICARE FRAUD PREVENTION: CMS HAS IMPLEMENTED A PREDICTIVE ANALYTICS SYSTEM, BUT NEEDS TO DEFINE MEASURES TO DETERMINE ITS EFFECTIVENESS 5–6 (2012), http://www.gao.gov/assets/650/649537.pdf [https://perma.cc/Q6RJ-AZ97].

175. GARRETT, *supra* note 46, at 271.

176. 2010–2011 FED. BUREAU OF INVESTIGATION FIN. CRIMES REP. 17, https://www.fbi.gov/file-repository/stats-services-publications-financial-crimes-report-2010-2011-financial-crimes-report-2010-2011.pdf/view[https://perma.cc/H9ND-NKCB].

177. *Id.* at 18.

and the BSA area, as well as others described, regulations and enforcers ask that companies conduct risk-based analysis in assessing the need for compliance. Thus, the DOJ called for "targeted audits" to test compliance procedure in the FCPA context.[178] The suggestion was that audits be targeted at areas posing special risks; for example, if particular countries were known to be high in corruption, or particular types of contractors thought to be less regulated or reliable, then audits would begin with those areas.[179] Compliance is not an all or nothing proposition, and compliance resources can be directed towards areas of risk.

E. Anonymous Reporting

Organizations can incentivize internal reporting of information. Prosecution agreements commonly provide for the creation of anonymous hot lines that employees may call.[180] Now Dodd-Frank, following a qui tam type model, financially rewards those who report to regulators,[181] but companies can and often do maintain internal systems aimed at encouraging reporting, precisely in hopes of avoiding external whistleblowing. Compliance offices may occasionally test these avenues by lodging sample complaints and tracking responses.[182] Whether employees actually employ these tip lines, or whether they instead fear retaliation, is itself an important question that can be investigated.

One method for examining the corporate climate and fear of retaliation is through employee surveys. Employee surveys are commonly used to assess how well officers and employees have retained training and policies. Such surveys may gauge employee perceptions and even understanding of training and policy, and they can be adapted to measure corporate climates, including assessments of how seriously supervisors take compliance issues and how they react to reports of problems. Employee surveys are not a reliable source of information about a respondent's own behaviors, because the employee may fear revealing conduct that could lead to adverse consequences, but surveys can be designed to elicit even reliable information about misconduct possibly observed within the company.[183] But such surveys, while useful, are no substitute for the tools described above that more directly probe for weaknesses in compliance mechanisms.

178. FCPA Resource Guide, *supra* note 85, at 58, 62.

179. *Id.*

180. GARRETT, *supra* note 46, at 77, 280.

181. *Id.* at 37, 226.

182. Eugene Soltes, *Paper Versus Practice: A Field Test of Integrity Hotlines*, 58 J. ACCT. RES. 429 (2020).

183. *See generally* Gregory Mitchell, *Employee Surveys on Sensitive Topics*, COMPLIANCE & ETHICS PRO. MAG., Sept. 2019, at 28.

VI
CONCLUSION

When is compliance effective? While enforcers emphasize that companies must adopt effective compliance, there is no focus on adoption of evidence-informed practices, much less well-done empirical validation of compliance. For a firm, it is unclear what compliance works, measuring compliance can result in liability, and liability itself is unclear due to an ill-defined compliance focus. As we have described, the path towards validated compliance in many areas, particularly those of greatest importance to lawmakers, regulators, and enforcers, is complicated and frustrated by the very enforcement priorities that produce the focus on compliance.

The compliance trap can be avoided. Government enforcers can create appropriate incentives for firms to develop and test best practices. In some areas, like the FCPA, private litigation cannot occur, making it more straightforward for regulators to privilege compliance and demand auditing of what works and what does not. In other areas, private litigation is likely, but compliance evidence will not likely play a great role in it. We have argued for a mandatory reporting regime designed to force companies out of the compliance trap, and we have described methods of testing compliance that can lead to more effective compliance programs, ultimately leading to lower litigation risks, both because misconduct becomes less frequent and because the company will have evidence that it undertook strong, validated compliance efforts.

If compliance were validated, we could design laws to better target the underlying problem. Enforcement could be more informed. Firms could more confidently invest in compliance. A validated compliance approach will hopefully increasingly emerge, but it will not do so organically. The compliance trap is too entrenched. Enforcers must jointly incentivize compliance and insist on validation and research. Legislators should consider how to do the same, or fund research on compliance. Independent research to validate forms of compliance is lacking. An organizational research agenda could benefit industry and the public, but it would have to begin with the appropriate incentives to overcome corporate fear that better data will bring liability. In an era of digital analytics, new and more powerful tools increasingly permit sophisticated analysis of organizational behavior. However, simple experiments, blind tests, random sampled audits, and other techniques, can test employee behavior at a very low cost.

Compliance programs seek to prevent some of the most socially harmful corporate conduct, but simply throwing money at compliance provides no guarantee of effective compliance. Compliance should be validated through empirical testing before it can be called effective. The focus of enforcement and regulation, ostensibly seeking to promote effective compliance, should be to reward the collection of compliance data and to harness the lessons from these data to improve corporate compliance. It will powerfully benefit both corporations and the public interest if we rigorously test compliance.