COLLABORATIVE GATEKEEPERS

Stavros Gadinis and Colby Mangels

ABSTRACT: In their efforts to hold financial institutions accountable after the 2007 financial crisis, U.S. regulators have repeatedly turned to anti-money laundering laws. Initially designed to fight drug cartels and terrorists, these laws have recently yielded billion-dollar fines for all types of bank engagement in fraud and have spurred an overhaul of financial institutions' internal compliance. This increased reliance on anti-money laundering laws, we argue, is due to distinct features that can better help regulators gain insights into financial fraud. Most other financial laws enlist private firms as gatekeepers and hold them liable if they *knowingly* or *negligently* engage in client fraud. Yet, as long as gatekeepers maintain deniability, they can accommodate dubious client requests. Instead, anti-money laundering laws require gatekeepers to report to regulators *suspicions* of misconduct, even without clear proof of fraud. Because suspicions arise early in the gatekeeper-client relationship, conflicts of interest are not likely to be as strong. Moreover, the task of identifying suspicious cases can be more readily outsourced to compliance departments, lessening dependence on front-line employees whose future might be tied to specific clients. Finally, suspicions may arise even in gatekeepers who only have partial access to clients' transactions, and thus cannot come to full knowledge of the fraud.

Inspired by the collaborative relationship between gatekeepers and enforcement authorities in anti-money laundering, we develop a theoretical framework that explains why this approach could operate as a general template for financial regulation. We then investigate the implementation of the collaborative model in practice. Starting from anti-money laundering laws' history, we present new evidence from recently released archival materials to illustrate that, rather than fighting proposals for expanding their regulatory obligations, private industry embraced them. Turning to the present, we discuss how the collaborative model has reshaped banking oversight in money laundering: it has leveraged the power of big data, encouraged the creation of dedicated compliance departments, and spearheaded one of the biggest inter-agency collaborations in the U.S. Finally, we discuss how the collaborative model could work in the future in two other areas of financial activity: broker-dealer regulation and equity issuance.

TABLE OF CONTENTS

I.

COLLABORATIVE GATEKEEPERS

Stavros Gadinis and Colby Mangels[*]

I. Introduction

In his annual letter to shareholders for 2014, Jamie Dimon, J.P. Morgan's CEO, made an astonishing revelation.[1] That year alone, his firm hired 8,000 new employees just to improve its compliance with anti-money laundering laws.[2] J.P. Morgan's recruitment zeal stemmed from a $2.6 billion penalty for anti-money laundering violations, due to its failure to spot Madoff's ponzi scheme.[3] This was hardly an isolated case:[4] anti-money laundering laws have played a central part in four out of the eight biggest fines in the wake of the financial crisis,[5] becoming a key legal basis in the quest to hold banks accountable. The newfound prominence of the

---

[*] Stavros Gadinis is an Assistant Professor at Berkeley Law School. Colby Mangels is a 2015 J.D. Graduate of Berkeley Law School. We would like to thank Kenneth Ayotte, Douglas Baird, Robert Bartlett, Omri Ben-Shahar, Dick Buxbaum, Anthony Casey, Steven Davidoff Solomon, Dhammika Dharmapala, Holly Doremus, David Gamage, Mark Gergen, Tom Ginsburg, Todd Henderson, William Hubbard, Saul Levmore, Jonathan Masur, Richard McAdams, Tom Miles, Randy Picker, Eric Posner, Julie Roin, Andrea Roth, Jonathan Simon, Lior Strahilevitz, Stephen Sugarman, and David Weisbach. We would like to acknowledge generous financial support from the Hellman Fund at UC Berkeley.

[1] J.P. MORGAN CHASE & CO., ANNUAL REPORT 2014 21 (2015), *available at* http://files.shareholder.com/downloads/ONE/3844439630x0x820077/8af78e45-1d81-4363-931c-439d04312ebc/JPMC-AR2014-LetterToShareholders.pdf.

[2] *Id*.

[3] The US Attorney's office struck a deferred prosecution agreement for an indictment of two years. Under the terms of this agreement, J.P. Morgan is required to reform its anti-money laundering compliance in accordance with a consent order issued by the Office of the Comptroller of the Currency. Consent Order, *In re* JPMorgan Chase Bank, N.A. *et al*. (No. 2013-002, U.S. Treasury Department, Jan. 14, 2013), *available at* http://www.occ.gov/news-issuances/news-releases/2013/nr-occ-2013-8a.pdf [hereinafter, DPA].

[4] Tom Braithwaite, Richard McGregor & Aaron Stanley, *Banks hit by $100bn in US legal settlements since crisis: - More than half paid in 2013 - Sum reflects shift in political attitudes*, FINANCIAL TIMES, March 26, 2014, at 1, *available at* http://www.ft.com/intl/cms/s/0/802ae15c-9b50-11e3-946b-00144feab7de.html.

[5] Stephen Grocer, *A List of the Biggest Bank Settlements*, MONEYBEAT, WALL ST. J., June 23, 2014., http://blogs.wsj.com/moneybeat/2014/06/23/a-list-of-the-biggest-bank-settlements/ (last visited Aug. 24, 2015). The cases against J.P. Morgan, BNP Paribas, HSBC, Credit Suisse, and UBS involved anti-money laundering violations, among others.

anti-money laundering framework is striking. These laws target drug cartels and terrorists, the criminal periphery of the financial system rather than its core weaknesses. But since 2007, the anti-money laundering framework has evolved into a critical detection and enforcement mechanism for regulators, and a key priority for private industry compliance.[6] So far, there is little in the legal literature that could explain this puzzling shift towards the anti-money laundering toolkit.[7]

This Article argues that regulators have turned to anti-money laundering because of distinct features that set it apart from other common bases of financial misconduct, such as the anti-fraud provisions of the federal securities laws. Most financial laws require financial institutions to identify misbehaving clients, imposing heavy liability when they *knowingly* or *negligently* fail to shut them out of the financial system. This liability threshold produces a perverse effect: market players are very careful to ensure that they never reach such knowledge or negligence. Instead of looking for signals of underlying fraud and investigating indications, our laws incentivize market players to turn a blind eye.

In contrast, anti-money laundering laws require private industry to share with authorities *suspicions* of misconduct, even when these pieces of information fall far short of proving illegality. This reporting obligation, we argue, can help financial intermediaries overcome conflicts of interest and motivates them to organize more effective compliance operations. In this Article, we explore this approach as a template for other areas of financial regulation. We develop a theoretical framework that explains the advantages of our proposed model, explore its history and application in anti-money laundering law, and discuss how it could operate in other fields.

Enlisting private firms as the primary line of defense against fraud and misconduct is the dominant strategy in financial regulation and is known as the "gatekeeper model." Gatekeepers are intermediaries whose cooperation is essential for many financial transactions: bankers, accountants, lawyers, credit rating

---

[6] *See infra* Part V.E.

[7] Legal scholarship on anti-money laundering laws focuses mostly on its criminal law dimensions. *See, e.g.,* William J. Stuntz, *Unequal Justice*, 121 HARV. L. REV. 1969, 1979-80 (2008) (arguing that money laundering's impact has been felt mostly against underprivileged groups); DOUGLAS HUSAK, OVERCRIMINALIZATION: THE LIMITS OF CRIMINAL LAW, 105 (2008) (arguing that money laundering is a case of overcriminalization); Samuel W. Buell, *The Upside of Overbreadth*, 83 N.Y.U. L. REV. 1491, 1537 (2008) (arguing that broader doctrine has assisted the federal government gain convictions); Richard G. Strafer, *Money Laundering: The Crime of the '90s*, 27 AM. CRIM. L. REV. 149 (1989) (discussing interpretative problems likely to arise after the criminalization of money laundering); Mariano-Florentino Cuellar, *The Tenuous Relationship Between the Fight Against Money Laundering and the Distruption of Criminal Finance*, 93 J. CRIM. L. & CRIMINOLOGY 311 (2003). For a discussion of the impact of money laundering's criminalization on the banking industry, see Sarah Jane Hughes, *Policing Money Laundering Through Funds Transfers: A Critique of Regulation under the Bank Secrecy Act*, 67 IND. L.J. 283 (1992) (discussing the burden of fund transfer policing for banks).

agencies, and other professionals.[8] Gatekeepers help address the informational asymmetries between investors and companies by verifying the credibility of contractual representations, be it the accuracy of financial statements, the risk profile of bonds, or the enforceability of legal claims. In theory, gatekeepers must maintain a reputation for integrity and should not be persuaded to participate in fraud just to win one client's fees. In many instances, laws supplement gatekeepers' reputational incentives with the threat of heavy sanctions.[9]

But as a spate of financial scandals has illustrated, gatekeepers have often found themselves involved in client fraud due to conflicts of interest between gatekeeper employees and their firms.[10] Gatekeeper employees are likely to have invested significant time and effort in building client relationships, and may not be willing to sacrifice a loss in compensation. Acquiescing to dubious client demands can be particularly tempting because the probability of detecting financial fraud is notoriously low. Fraudulent schemes do not look very different from legitimate profit-making transactions. Victims often do not realize that they have been misled until their investment has evaporated and perpetrators have disappeared or are unable to repay. Moreover, the sheer volume and sophistication of modern transactions make the financial system very hard to police. Without an inside tip about fraud, regulators seem reduced to playing catch-up; they often fail.[11]

Recognizing that information from the inside is essential in combatting financial fraud, policymakers have tried various strategies for strengthening gatekeepers' incentives to come forward. Sarbanes-Oxley enacted measures to insulate accountants from the pressures of corporate executives, but in most cases weaknesses in companies' financial statements remained unreported.[12] Dodd-Frank provides some whistleblowers a share of the bounty, but does not extend this offer to professionals required to report misconduct to regulators under other rules.[13] Academics have also debated how to beef up the gatekeeper regime. Prominent proposals involve making gatekeepers strictly liable for client misconduct up to a

---

[8] *See* Reiner H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J. L. ECON. & ORG. 53, 54 (1986) (defining gatekeepers as "private parties who are able to disrupt misconduct by withholding their cooperation from wrongdoers."). *See also infra* Parts II.A-C (discussing the literature on gatekeepers).

[9] *See infra* Part II.A.

[10] *See* JOHN C. COFFEE, JR., GATEKEEPERS: THE ROLE OF THE PROFESSIONS AND CORPORATE GOVERNANCE 5 (2006); John C. Coffee, Jr., *Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms*, 84 B.U. L. REV. 301, 308 (2004).

[11] *See infra* Part II.B.

[12] *See generally* John C. Coates IV, *The Goals and Promise of the Sarbanes-Oxley Act*, 21 J. ECON. PERSP. 91, 96 (2007). (discussing the motivations behinds Sarbanes-Oxley and reviewing empirical evidence regarding its performance in practice); see also *infra* Part II.C.1.

[13] Section 21F(2)(C) of the Securities Exchange Act of 1934, 48 Stat. 881 (1934) (codified at 15 U.S.C. § 78u-6(c)(2)(C)(2012)), hereinafter 1934 Act. *See also infra* Part II.C.2.

capped amount. But there are fears that such an expansion of liability would place too high a burden on the industry and push out legitimate clients.[14]

This Article explores an alternative design for structuring gatekeepers' obligations, which can help overcome many of the above problems and provide regulators with more information on potential fraud. Imagine requiring gatekeepers to report not positive knowledge, but *suspicions* of illegality. In their dealings with clients, gatekeepers may come to realize that there are gaps in a client's rationale for pursuing a transaction, or that the information the client provides does not add up. Alternatively, a client's conduct might be very unusual, or have much in common with past instances of client fraud. Such indications of potential illegality are information that gatekeepers can collect and pass on to authorities. In return, regulators could guarantee the anonymity of the report, so as not to disrupt the gatekeeper-client relationship should the transaction turn out to be legitimate.

Setting the reporting threshold at the level of suspicions, rather than knowledge, can radically change gatekeepers' incentives and improve the effectiveness of regulatory interventions. Suspicions are bound to arise at a much earlier stage in the gatekeeper-client relationship, when the resources invested in building this relationship are lower, and the bond of loyalty between the two parties is not as strong. Some client proposals may trigger suspicions even before gatekeepers actually start offering any services. Consequently, the conflicts of interest that gatekeepers are likely to face will be weaker. Moreover, regulators may be able to combine multiple reports on a single client or transaction and take preventive actions even if each gatekeeper has come to know only part of the client's activities or dealings.[15] Because of the close interactions between gatekeepers and regulators, we term this approach "collaborative gatekeeping."

To change industry attitudes towards client cover-ups, the law should provide for sanctions against gatekeepers who fail to submit a report. The threat of sanctions can motivate gatekeepers to establish internal systems for identifying suspicious cases, train front-line employees to be alert about potential fraud, and draft reports.[16] Importantly, sanctions underline that suspicious activity reporting is a regulatory obligation enforceable against everyone in the financial industry. As all gatekeepers flock to submit reports, the stigma associated with providing client information to regulators is likely to fade away.[17]

Gatekeepers will be more likely to submit reports if they gain immunity against enforcement actions arising out of the information they provide. Immunity will allow gatekeepers to continue working with the client even after the report without immediately foregoing all future revenue when a transaction is legitimate, tempering further the impact of conflicts of interest. Immunity also shields gatekeepers from the risk of self-incrimination, if an ensuing investigation reveals that their firm's involvement in client fraud was greater than initially suspected. Thus, immunity removes important inhibitions gatekeepers may have and offers

[14] *See infra* Part II.C.3.
[15] *See infra* Parts III.A-B.
[16] *See infra* Part III.C.
[17] *See infra* Parts III.E-F.

greater benefits upon providing information. That said, immunity should extend to gatekeepers only as long as they continue to act in good faith.[18]

While these arguments underscore the theoretical appeal of the model, there might be doubts as to its workability. One set of worries might focus on the political economy of financial regulation. Private industry might choose to oppose the expansion of its regulatory obligations and the additional effort and resources it entails. Another set of questions might concern the promised informational upside. The financial industry might choose to stick with client loyalty and refuse to embrace suspicious activity reporting. Or, in the exact opposite scenario, finance professionals might flood regulators with reports about clients' activities, providing incomplete information about countless cases that authorities could not possibly analyze or pursue any further.

We can shed some light on these concerns by looking at anti-money laundering law, which, due to a historical happenstance, follows closely the theoretical model outlined above. While the conventional gatekeeper model is deeply embedded in U.S. law, the anti-money laundering regime has its origins in 1970's Switzerland, from where it spread around the world, including the U.S.[19] Taking advantage of archival materials released publicly from the Swiss central bank for the first time after 40 years, the Article brings to light the motivations of the regime's inspirers and the contributions of key players, such as financial institutions and industry associations. Our exploration of the historical record reveals collaborative gatekeeping as a rare case of a regulatory scheme that the industry chose to embrace, rather than bitterly oppose. Of course, the industry's consent did not come without concessions from regulators, such as standardized, objective criteria for suspicions and universal application to all market participants. Moreover, the spread of collaborative gatekeeping as a template for anti-money laundering laws around the world shows that stricter laws do not necessarily place a national market in a competitive disadvantage, but can trigger parallel developments elsewhere.

A unique constellation of enforcement bodies and market players have seen the value of intelligence gathered through the anti-money laundering regime and launched large-scale collaborations aided by cutting-edge technology. Over 1.5 million suspicious activity reports reach the Treasury Department annually. Institutions across the financial industry have espoused suspicious activity reporting, from banks to brokerages to wire services, from big financial powerhouses to small community ventures, from urban centers to rural areas. To fulfill their obligations, private firms have revolutionized their compliance operations and introduced digitalized systems using "bid data" approaches. All this private industry activity shows how the collaborative model can effectively change market-wide attitudes. In turn, these reports have helped regulators pursue a wide range of financial and criminal misconduct beyond money laundering, including tax evasion, mortgage fraud, and insider trading. Financial regulators such as the Federal Reserve and the SEC, as well as government agencies such as the IRS and the

[18] *See infra* Part III.D.

[19] *See infra* Part IV.A.

Department of Justice, have expanded their oversight operations to better take advantage of gathered intelligence. Over one hundred review teams from these agencies pore over the reports in weekly or monthly meetings, while the Treasury also operates a central database that is open to hundreds of local and state authorities.

The first two parts of the article outline its theoretical contributions, presenting collaborative gatekeeping as a coherent model for enlisting the help of financial intermediaries in enforcement. Part II below discusses the analytical foundations of the current gatekeeping regime and the problems associated with conflicts of interest. Part III delineates collaborative gatekeeping as a theoretical model, explores its key elements, and discusses how it could help blunt the conflicts of interest that plague gatekeepers. The remaining parts of the article discuss the application of collaborative gatekeeping in the case of anti-money laundering law, and explore the potential extension of the model to other areas of financial regulation. Part IV shows how regulators and private industry worked together to complete the anti-money laundering regime over time, first in Switzerland, and then at the international level under U.S. leadership. Part V presents some tentative evidence about the operation of the anti-money laundering regime in the U.S. Part VI discusses how the principles of collaborative gatekeeping could work in the context of broker-dealer regulation and securities issuance. Part VII concludes.

II. Gatekeepers in Current Theory and Practice

A. The Theory of Gatekeeping – Market-Based Regulation Through Reputation

Financial transactions typically involve a professional intermediary: investment bankers, accountants, and lawyers help companies issue securities to the public; retail banks help long-term borrowers access funding from short-term depositors; rating agencies assess bonds' risk of default on behalf of buyers; and so on. For investors wary about their money, these professionals' stamp of approval can turn a risky investment into a legitimate business proposition, rather than a venture into the unknown. In turn, businesses seek these professionals' help to boost their appeal to investors and gain access to a wider pool of funds. By facilitating a transaction, these professionals open the gates of the financial system to new entrants; thus, they are termed "gatekeepers."[20] Enlisting gatekeepers in the fight against fraud and misconduct is the most prominent strategy across many different fields in modern financial regulation. This strategy, premised on gatekeepers' desire to keep their reputation pristine, has received much attention by scholars and policymakers alike. The following paragraphs outline the reputation-based theory of gatekeeping, while subsequent sections explore the

[20] *See* Kraakman, *supra* note 8.

limitations of this reputation based- approach, and regulatory reforms and academic proposals intended to place greater liability on gatekeepers.

As intermediaries in many transactions, gatekeepers occupy a unique place in the market. Because of their close connections with clients, gatekeepers are better informed than regulators regarding the goals, intentions, and underlying financial realities of client firms.[21] Due to this informational advantage, the market looks at gatekeepers to verify the disclosures, risk profile, or general quality of financial instruments offered in a transaction. Gatekeepers command markets' trust because, over time, they have built significant reputational capital, by verifying transactions and statements that have repeatedly proven accurate.[22] Their business model relies on maintaining and augmenting this reputational capital; without it, they can no longer perform their verification role. Certainly, gatekeepers receive hefty fees for their verifications, which they stand to lose if they do not cooperate with a client's fraudulent scheme. But if gatekeepers' role in a fraudulent transaction is found out, they stand to lose all credibility with the market and thus all future business. This risk is so great, it is thought, that no single client's fee payment can possibly compensate for it.[23] For these reasons, conventional wisdom holds that gatekeepers will not sacrifice their reputation and future profits to satisfy any individual client's requests, however well the client pays.

Gatekeepers' verification function is also the basis for their role in enforcement. If gatekeepers realize that their client is violating the law, they can withhold their approval and prevent this wrongdoer from entering the financial system. Taking advantage of this power, the law has often required mandatory gatekeeper participation in transactions plagued by significant information asymmetries, such as securities offerings. In those cases, the law has imposed on gatekeepers a duty to examine each client's conduct and credentials.[24] To back this duty, the law establishes harsh penalties against gatekeepers that fail to catch misconduct on their watch. Gatekeepers must compensate victims of their clients' fraud unless they satisfy demanding defenses. In addition to investor-driven enforcement, gatekeepers are also subject to sanctions by regulators, such as fines or bans from the industry.

The main function of this regime is to deter gatekeepers from acquiescing to fraudulent activities.[25] In order to avoid these penalties, it is hoped, gatekeepers will monitor their clients closely and steer them away from misconduct through their advice. Kraakman aptly called this type of gatekeeper a "chaperone:" someone who, as the relationship with a client unfolds, intervenes to prevent a violation from happening, realigning the client's actions so that they fall within the requirements of the law.

In this conception of gatekeeping, regulation plays a limited role, besides brandishing the threat of sanctions. If everything works as intended, gatekeepers

---

[21] Coates, *supra* note 12.
[22] Coffee, Jr.,*Gatekeeper Failure, supra* note 10, at 308.
[23] *Id.*
[24] Kraakman, *supra* note 8, at 53.
[25] Sung Hui Kim, *Gatekeepers Inside Out*, 21 GEO. J. LEGAL ETHICS 411, 423 (2008).

will either discipline misbehaving clients or cut them off from the financial system before fraud is committed. In both cases, harm to third parties is averted, so there is little reason to involve enforcement authorities. Although the law expects gatekeepers to monitor their clients and direct their activities, it provides neither any guidance nor any tools to help them achieve these goals. Gatekeepers' reputational incentives and fear of sanctions are thought to provide enough motivation; gatekeepers' close knowledge of client workings ensures they are best positioned to deal with attempted misconduct; finally, gatekeepers' market power leaves clients with no other option but to follow gatekeepers' recommendations. Essentially, regulators are expected to intervene only *ex post*, in the rare event that something in the gatekeeper-client relationship goes amiss.

B. The Harsh Realities of Gatekeeping: Repeated Collapses Show Weaknesses in Reputational Model

In practice, neither reputational incentives nor the deterrent effect of harsh sanctions have managed to discipline gatekeepers, as the last fifteen years of financial turmoil have shown. In 2001, Enron collapsed when it was revealed that its management had successfully pressured its outside accountant, Arthur Andersen, to overlook liabilities hidden through off-balance-sheet transactions.[26] But if Enron's deceptions were masterfully designed, Worldcom's fraud was much more mundane: its CFO, in cooperation with its outside accountant, Arthur Andersen (again), simply misclassified expenses and inflated revenues.[27] While Enron and Worldcom are the most famous examples of large-scale accounting irregularities, they were not the only ones.[28] Nor were accountants the only gatekeepers found to succumb to such conflicts of interest. In 2003, securities analysts, who write independent reviews of securities offerings and issue buy-sell-hold recommendations, were found to

---

[26] David Henry et al., *Who Else Is Hiding Debt*, BUS. WK., Jan. 27, 2002, at 36-37, *available at* www.bloomberg.com/bw/stories/2002-01-27/who-else-is-hiding-debt; Jonathan Weil, *How Leases Play A Shadowy Role In Accounting*, WALL ST. J., Sept. 22, 2014, at A1, *available at* www.wsj.com/articles/SB109580870299124246.

[27] Simon Romero and Alex Berenson, *WorldCom Says It Hid Expenses, Inflating Cash Flow $3.8 Billion*, N.Y. TIMES, June 26, 2002, at A1, *available at* http://www.nytimes.com/2002/06/26/technology/26TELE.html.

[28] *See, e.g.,*Daniel J.H. Greenwood, *Enronitis: Why Good Corporations Go Bad*, 2004 COLUM. BUS. L. REV. 773, 786; *see also* Andrew Ross Sorkin, *2 Top Tyco Executives Charged With $600 Million Fraud Scheme*, N.Y. TIMES, Sept. 13, 2002, at C1, *available at* www.nytimes.com/2002/09/13/business/2-top-tyco-executives-charged-with-600-million-fraud-scheme.html (discussing the Tyco International Ltd. racketeering scheme); *see also Ahold: Europe's Enron*, ECONOMIST, Mar. 1, 2003, at 63, *available at* http://www.economist.com/node/1610552 (discussing the Royal Ahold scandal); *see also* Claudio Storelli, *Corporate Governance Failures - Is Parmalat Europe's Enron?*, 2005 COLUM. BUS. L. REV. 765 (discussing the Parmalat scandal).

overwhelmingly favor companies that had hired the analyst's employer to run the offering[29] after being promised under-the-table rewards.[30]

The financial crisis of 2007-2008 brought to light a new set of gatekeeper missteps. To successfully repackage and sell mortgage-backed securities, investment banks represented to buyers that their products had a much lower risk profile than the one eventually revealed once the subprime market collapsed.[31] Credit rating agencies, hired by investment bankers to conduct an independent assessment of the securities' risk profile, contributed to the collective euphoria by downplaying the possibility of default. In the midst of this upheaval, Bernie Madoff, a well-respected financier and former head of NASD, shockingly confessed to running an estimated $50 billion Ponzi scheme. For decades, Madoff's fraud continued under the nose of the nation's biggest bank, JP Morgan. In 2014, JP Morgan agreed to a hefty $2.6 billion in monetary sanctions for failing to alert regulators about the Madoff case.[32]

These events dominated national headlines, attracted enormous scholarly attention, and triggered important legislative and regulatory reforms.[33] While each of these cases involved distinct failures, they also underscore fundamental weaknesses in the conventional gatekeeper model. Gatekeepers, it turned out, sometimes went out of their way to keep their clients satisfied, even when this meant disregarding indications of potential fraud. After all, the probability that clients' fraud will be detected is relatively low. And even when fraud is revealed, our laws often allow gatekeepers to avoid liability if they were not aware of it, or at least not negligent in ignoring it. Below we explain why our current laws have allowed the conflicts of interest in gatekeeping to burgeon in light of the low probability of detecting fraud.

---

[29] Jill E. Fisch and Hillary A. Sale, *The Securities Analyst as Agent: Rethinking the Regulation of Analysts*, 88 IOWA L. REV. 1035, 1037 (2003).

[30] Press Release, Securities and Exchange Commission, Ten of Nation's Top Investment Firms Settle Enforcement Actions Involving Conflicts of Interest Between Research and Investment Banking (Apr. 28, 2003), *available at* http://www.sec.gov/news/press/2003-54.htm.

[31] *See* SEC v. Goldman Sachs & Co., 790 F. Supp. 2d 147 (S.D.N.Y. 2011) (presenting SEC allegations that Goldman Sachs misrepresented to investors in ABACUS vital information about the risk profile and portfolio selection process).

[32] Walter Hamilton & Stuart Pfeifer, *JPMorgan to Pay $2.6 Billion for Failing to Report Madoff Concerns*, LOS ANGELES TIMES, Jan. 08, 2014, at B1, *available at* www.articles.latimes.com/2014/jan/07/business/la-fi-jpmorgan-madoff-20140108.

[33] For examples of legislators calling for reform following the Madoff scandal, see Liz Moyer, *Can New Regulation Stop Another Madoff?*, FORBES, Jan. 5, 2009, www.forbes.com/2009/01/05/madoff-regulation-banking-biz-wall-cx_lm_0105madoff.html; *The Securities and Exchange Commission Post-Madoff Reforms*, S.E.C. http://www.sec.gov/spotlight/secpostmadoffreforms.htm (last updated Apr. 2, 2012).

1. The Conflicting Interests of Gatekeeper Firms and Their Employees

In the eyes of the law, ideal gatekeepers are sizeable corporations that boast a strong reputation won after decades of experience, command large market shares in their industry, and employ thousands of professionals. With such leverage, gatekeepers have little reason to acquiesce to devious client demands. Behind the firm's façade, however, deals are struck between individual professionals and client executives. Some gatekeepers, such as certain investment banks or law firms, operate on the basis of "eat what you kill" models, where each professional's compensation or bonus depends on the billings she brings to the firm.[34] But even in firms that do not keep strict tally of the loot, gatekeeper professionals are in charge of specific client accounts, which they are expected to cultivate and grow.[35] Thus, a gatekeeper professional's annual pay and future in the firm may depend entirely on a few clients, or even on a single one. These clients may only represent a sliver of the firm's aggregate billings, but mean the world to the individual professional who caters to their needs. Forging these client relationships requires significant time and effort from gatekeeper professionals, and building trust with clients may take years. When such a profitable client relationship is lost, it could take considerable time for the professional to identify and develop a suitable alternative.[36] Moreover, long-term relationships between gatekeeper professionals and client executives often start as staid business transactions but develop into personal friendships. Sentiments such as trust, loyalty, and affinity become the basis for lasting and rewarding interactions.[37]

So, if these valued clients and trusted friends ask the individual professional to cooperate with them and violate the law, will she be willing to go along, or will she resist? In the cases examined above, the short-term incentives of personal enrichment won over the long-term goals of maintaining the firm's reputational capital, or even its continued existence.[38]

Apart from specific considerations generated by gatekeepers' investment in client relationships, market-wide norms paint cooperating with authorities as betrayal of one's own clients. In tightly regulated industries, such as finance,

---

[34] For "eat what you kill" models in the banking industry, see Suzanne McGee, *'You Eat What You Kill': Wall Street Bonuses Keep Soaring as Profits Decline*, THE GUARDIAN US MONEY BLOG (Mar. 15, 2015), www.theguardian.com/money/us-money-blog/2015/mar/15/wall-street-bonuses-rise-profits-decline. For "eat what you kill" in law firms settings, see Milton C. Regan, Jr. & Lisa H. Rohrer, *Money and Meaning: The Moral Economy of Law Firm Compensation*, 10 U. ST. THOMAS L.J. 74, 115 (2012).

[35] Kim, *supra* note 25, at 432-33.

[36] Lawrence A. Cunningham, *Beyond Liability: Rewarding Effective Gatekeepers*, 92 MINN. L. REV. 323, 350 (2007).

[37] Sung Hui Kim, *The Banality of Fraud: Re-Situating the Inside Counsel as Gatekeeper*, 74 FORDHAM L. REV 983, 1057 (2005-2006).

[38] Merritt B. Fox, *Gatekeepers Failures: Why Important, What to Do*, 106 MICH. L. REV 1089, 1103 (2007-2008).

regulators are often seen, if not exactly as the "enemy," but as someone whose gaze is best avoided.[39] Moreover, informing enforcement authorities about somebody else's misconduct carries negative social connotations: informants are labeled snitches.[40] In service industries that prize loyalty above all else, working with regulators against one's own clients is often seen as the ultimate betrayal. Stigmatized by their actions, these gatekeepers are seen as unfaithful agents who put their own interest ahead of their client's, as overly sensitive to their regulatory obligations, as unpredictable and untrustworthy collaborators who will not protect their client at moments of crisis. Gatekeepers whose reputation is thus tainted have trouble attracting business, and may have to abandon the industry.

2. The Low Probability of Detecting Fraud

Modern finance is an exceedingly technical environment, with layers of intermediaries interacting through complicated transactions using ever more refined instruments with diverse motivations. Highly knowledgeable market participants take advantage of this complexity, typically to make legitimate gains, but sometimes to devise intricate fraud schemes. However deep the machinations behind fraud run, the outcome is often similar: the probability of detecting financial fraud is often very low.

But surely, one might think, at some point the fraudulent edifice will collapse, the harm done to victims will be revealed, and enforcement will restore order. While true for most crimes or torts, this proposition does not necessarily stand for financial fraud. Some financial crimes take place in order to address presumably short-term problems, such as a liquidity crunch or a temporary market downturn, with the intention of replenishing misappropriated funds once things look up.[41] Other fraudulent schemes are designed to continue in perpetuity and can even withstand some disturbances. Madoff successfully run his Ponzi scheme for decades, and he finally revealed it himself. In still other cases, misconduct has a clearly harmful impact for markets' credibility, but pinpointing specific losses and connecting them to specific victims might be impracticably difficult because of the

[39] Illustrative of this point: in a speech delivered by Xerox Corporation's CEO at an SEC conference, the CEO joked that all CEOs feel strange when entering the SEC building. *See* Anne M. Mulcahy, Remarks at the SEC Interactive Data Roundtable Panel on Getting Analyst and Investors Significantly Better Information 109 (June 12, 2006) (transcript available at www.sec.gov/spotlight/xbrl/xbrlofficialtranscript0606.pdf).

[40] Naseem Faqihi, *Choosing Which Rule to Break First: An In-House Attorney Whistleblower's Choices After Discovering a Possible Federal Securities Law Violation*, 82 FORDHAM L. REV. 3341, 3349-51 (2014).

[41] *See*, *e.g.*, Matthew O'Brien, *Meet the Most Indebted Man in the World*, ATLANTIC, Nov. 2, 2012, www.theatlantic.com/business/archive/2012/11/meet-the-most-indebted-man-in-the-world/264413 (discussing Jerome Kerviel, Société Générale rogue trader).

sheer number of victims harmed just a little.[42] Finally, some fraudulent schemes take advantage of a systemic weakness that affects all market participants in one way or another, as was the case with the security analysts' conflicts of interest. For all these reasons, identifying or even conceptualizing victims might be exceedingly hard. When the victims themselves do not have a clear sense of harm, they are unlikely to point authorities to the fraud and demand action.

The low probability of detecting financial fraud further sharpens the conflict of interest between gatekeeper firms and employees discussed above. Motivated by short-term gains, such as increased compensation, better reputation, and professional advancement, employees might be more tempted to disregard warning signs if they believe no one is going to find out. Succumbing to misguided client requests is easier, if the probability of being discovered is really low. Moreover, employees might have pocketed their gains and left the firm by the time the effects of the fraud fully unfold. Whether these individuals' assets will be available for compensating fraud victims depends on doctrines of gatekeeper fault, which often raise hurdles.[43] In practice, sanctions against individual employees are rare.[44]

Economic theory suggests that, when the probability of detection is low, policymakers can still deter harmful conduct successfully with a substantial increase in sanctions.[45] However, increasing sanctions might not be a viable option in the case of gatekeeper misconduct. To start, market reaction to severe gatekeeper fault can be immediate and overwhelming, as Arthur Andersen's collapse after Enron illustrates. When the gatekeeper firm dissipates, there are really no additional sanctions that policymakers can impose. Moreover, our regulatory framework utilizes gatekeepers to such an extent that eliminating them through harsh sanctioning might leave the market even more exposed to misconduct than before. The global financial system relies on just four big accounting firms and three credit rating agencies, and many fear about the already diminished levels of competition among them.

Yet, it is because of the low probability of detection that gatekeeper collaboration is absolutely essential in any effort to uproot fraud. Many of the recent headline financial scandals have come to light or reached resolution because someone with direct knowledge of the scheme worked with enforcement authorities. In Worldcom, it was internal accountants that unearthed the scheme; in Goldman's Abacus deal, it was months of interviews with industry insiders that

---

[42] In the market-timing scandals, the losers where the people who traded right before the close of the market. *See* James Surowiecki, *Right Trade, Wrong Time,* THE NEW YORKER, Oct. 20, 2003, at 74, *available at* www.newyorker.com/magazine/2003/10/20/right-trade-wrong-time.

[43] *See infra* Part II.B.3.

[44] Stavros Gadinis, *The SEC and the Financial Industry: Evidence from Enforcement Against Broker-Dealers*, 67 BUS. LAW. 679, 682 (2012).

[45] A. Mitchell Polinsky & Steven Shavell, *The Theory of Public Enforcement of Law*, *in* HANDBOOK OF LAW AND ECONOMICS 403, 427-29 (A. Mitchell Polinsky & Steven Shavell eds., 2007).

allowed the Securities and Exchange Commission to zero in on this particular deal;[46] Enron's Andrew Fastow,[47] and, of course, Bernie Madoff,[48] offered up themselves to authorities. Inside information can save a lot of effort and resources for regulators by directing them right to the target. Gatekeepers are uniquely placed to provide such direction, because they are sophisticated professionals who understand the intricacies of the financial system and can spot signs of misconduct. But instead of enlisting their cooperation in finding out more about fraud, our laws steer them towards knowing as little as possible about it so as to avoid liability, as the next section argues.

3. For Gatekeepers, Knowledge is Liability

Gatekeeper liability is not strict. Rather, to be liable toward victims of their clients' misconduct, or subject to regulatory sanctioning, gatekeepers must have violated a duty specifically prescribed by law.[49] In defining these duties, the law typically requires that gatekeepers either intend to or at least know that their actions violate the law. Take for example Rule 10b-5, the catch-all definition of securities fraud that has allowed investors to launch thousands of private claims against investment banks, accountants, and lawyers. A key element of 10b-5 fraud is scienter,[50] satisfied when the information that the defendant possesses allows her to know or reasonably foresee the potential result of her action.[51] In the same vein, the Securities Exchange Act of 1934 authorizes the Securities and Exchange Commission to suspend or revoke the operating license of broker-dealers when they willfully violate, or aid and abet in violating, securities laws.[52] On the banking side, liability arrangements are similar. For example, the billion-dollar fines that banks have paid for misrepresenting the value of mortgage portfolios in the run-up to the 2008 crisis are based on FIRREA.[53] Since FIRREA civil penalties arise in case of mail and wire fraud that harms federally insured financial institutions, they also require scienter.

---

[46] Louise Story & Gretchen Morgenson, *S.E.C. Accuses Goldman of Fraud in Housing Deal,* N.Y. TIMES, Apr. 16, 2010, at A1, *available at* http://www.nytimes.com/2010/04/17/business/17goldman.html.

[47] Jen Rogers, *Fastow and His Wife Plead Guilty*, CNNMONEY, Jan. 15, 2004, www.money.cnn.com/2004/01/14/news/companies/enron_fastows.

[48] Scott Cohn, *Madoff Says He Provided 'Key Information' to Authorities*, CNBC, Dec. 13, 2013, www.cnbc.com/id/101272415.

[49] Jennifer Arlen & Reinier Kraakman, *Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes*, 72 N.Y.U L. REV. 687, 697 (1997).

[50] Ernst & Ernst v. Hochfelder, 425 U.S. 185, 202 (1976).

[51] AUSA Life Insurance Co. v. Ernst & Young, 206 F.3d 202 (2d Cir. 2000).

[52] 1934 Act § 15(b)(4)(D)–(E), 15 U.S.C. § 78*o*(b)(4)(D)–(E) (2012).

[53] Financial Institutions Reform, Recovery, and Enforcement Act of 1989 § 951, 18 U.S.C. § 1833a (2012) [hereinafter, "FIRREA"].

Tying gatekeeper liability to knowledge of illegality has an important perverse effect that has been largely overlooked by the literature.[54] If a gatekeeper is not held liable unless it knows about client mischief, then the less it knows about the client, the more likely it is that the gatekeeper will avoid liability altogether. By maintaining a position of unawareness, gatekeepers can continue offering services to and collecting fees from clients that are engaging in illegalities. In this way, gatekeepers caught between their client loyalties and their regulatory obligations can satisfy both masters. Thus, rather than pursuing their market-monitoring role to the fullest, gatekeepers are actually better off by averting their gaze, so that they limit the chances of coming across information that would compromise their unawareness. Only when they cannot plausibly deny knowing about clients' scheming are gatekeepers forced to abandon their neutrality. As a result, indications that are likely to signal misconduct, but do not positively prove it, might often be left unexplored.

In few notable cases, gatekeeper liability departs from scienter and employs a negligence standard, as is the case for inaccuracies in a registration statement for underwriters, accountants, attorneys, and others under §11 of the 1933 Act. Courts are left with the challenging task of defining what constitutes reasonable care in each case, a rather costly and complicated exercise that typically entails significant uncertainty for all parties involved.[55] To reach this determination, courts typically refer to the standards of due diligence in the relevant professional setting, and invite expert testimony on whether the defendant took all the appropriate steps to investigate and assess the situation at hand.[56] Defendants are found liable if they continue to work with clients that their peers would have cut off from the financial system and referred to enforcement authorities. Recent cases have added more bite to this due diligence exercise, requiring that gatekeepers consider "red flags," i.e. facts that put the defendant on notice that the client is engaged in wrongdoing, or that would suggest to the average investor that she has been defrauded.[57] Red flags must "strip a defendant of his confidence" in the accuracy of his clients' representations.[58] Although less demanding than scienter, this negligence standard still requires gatekeepers to turn away their clients only after evidence starts mounting against them. Thus, it still leaves gatekeepers significant space to accommodate client demands before they run into trouble.

Before information about client misconduct reaches the level of scienter or negligence, gatekeepers have no legal obligation to alert regulators, and very little reason to do so voluntarily. If gatekeepers terminated their engagement based on

---

[54] Note that Professor Jennifer Arlen makes a similar point for corporate liability regime for employees' torts and crimes. *See* Jennifer Arlen, *The Potentially Perverse Effects of Corporate Criminal Liability*, 23 J. LEGAL STUD. 833 (1994).

[55] Assaf Hamdani, *Gatekeeper Liability*, 77 S. CAL L. REV. 53, 59 (2003).

[56] *See, e.g.*, Danis v. USN Commc'n, Inc., 121 F. Supp. 2d 1183 (N.D. Ill. 2000); Wikoff v. Vanderveld, 897 F.2d 232, 235 (7th Cir. 1990); *In re* Discovery Zone Sec. Litig., 943 F.Supp. 924, 935 (N.D. Ill. 1996).

[57] *In re* Worldcom, Inc. Sec. Litig., 346 F. Supp. 2d 628, 672–73 (S.D.N.Y. 2004).

[58] *Id.* at 674.

unverified suspicions, their relationship with the clients in question would probably be irreparably damaged, and their reputation in the market would suffer. If gatekeepers reported their suspicions to regulators, the transaction would probably stall or be canceled and the client may suffer as a result. Again, gatekeepers put the opportunity to collect fees for their services at risk, and might even find themselves targeted in an enforcement action. As a result, gatekeepers often find themselves tiptoeing around the red line of illegality, putting up a shield around their own liability, rather than worrying about the impact of their clients' actions for third parties and the financial system as a whole.

Even when revelation of the fraud is imminent and the delicate balancing act between satisfying client demands and complying with regulatory obligations is about to crumble down, we have seen gatekeepers trying to protect their position by concealing evidence. At least in past financial scandals, gatekeepers had in fact gone to great lengths to keep authorities in the dark: for example, they obstructed evidence,[59] got the cooperation of other gatekeepers in the transaction[60] and even created secret code words and reference schemes.[61] By misdirecting gatekeepers' efforts in this way, our regulatory framework loses the chance to fully capitalize on their role as intermediaries and collect valuable intelligence that could help with enforcement.

C. Attempts At Reform: Sarbanes-Oxley and Dodd-Frank

As successive waves of financial scandals drove the economy into a tailspin, Congress made repeated efforts to reform the gatekeeper model. While these reforms targeted only certain types of gatekeepers, each represents a different strategy that could be applied to gatekeeping more generally. More specifically, Congress tried two new approaches. First, it sought to instill greater discipline from the inside; it created procedures that streamline gatekeepers' due diligence obligations and supervisory mechanisms. This set of measures is mostly associated with the 2002 Sarbanes-Oxley Act, which used this approach in relation to financial statement audits. Second, Congress offered increased rewards to gatekeepers who

---

[59] See United States v. Arthur Andersen, LLP, 544 U.S. 696, 701 (2005) (discussing the shredding of documents by auditor Arthur Andersen in the midst of the SEC investigation of Enron). *See also* Samuel W. Buell, *The Blaming Function of Entity Criminal Liability*, 81 IND. L.J. 473 (2006) (discussing various gatekeepers' efforts to shield clients and proposing entity criminal liability).

[60] Stoneridge Inv. Partners, LLC v. Scientific-Atlanta, Inc., 552 U.S. 148, 152 (2008) (discussing the liability of a gatekeeper who had not made a public misstatement or violated a duty to disclose, but had participated in a scheme to assist fraudsters). *See also* Anthony Sallah, *Scheme Liability: Conduct Beyond the Misrepresentations, Deceptive Acts, and Possible* Janus *Intervention*, 45 U. TOL. L. REV. 181 (2013).

[61] *See Collusion in the Stockmarket*, ECONOMIST, Jan. 15, 1998, at 89, *available at* www.economist.com/node/111273.

decide to "blow the whistle" on their employers. Although Sarbanes-Oxley also included whistleblower provisions, it was the 2010 Dodd-Frank Act that revolutionized and greatly expanded this approach. The paragraphs below look briefly at these reforms as models for regulating gatekeepers, arguing that there is still more to be done.

1. Sarbanes-Oxley: Intensifying Due Diligence and Increasing Independence from Management

Troubled by accountants who either actively collaborated with misbehaving managers, or turned a blind eye toward them, the Sarbanes-Oxley Act established a new regime to govern the interactions between public companies and their external auditors. The Sarbanes-Oxley regime orchestrates accountants' due diligence obligations extensively. The Public Company Accounting Oversight Board (PCAOB), a new quasi-public regulator, issues Audit Standards that specify steps and criteria external accountants must follow when auditing public companies. By directing accountants' attention to many different inquiries, the Sarbanes-Oxley regime makes it harder for them to claim that they failed to notice problems. Moreover, Sarbanes-Oxley's section 404 requires auditors to review not only the company's financial statements, but also the systems that the company has in place in order to collect the information used to produce the financial statements. Thus, it expands the scope of accountants' inquiries even further.

But if these expanded inquiries unearth problems, what are accountants to do? Sarbanes-Oxley sets up two new channels that accountants can use to pursue their complaints, one within the corporate hierarchy and one outside it. First, accountants can bring up their concerns with the audit committee, a specialized board committee composed entirely of independent directors. Responsible for hiring and firing auditors, as well as for supervising the company's internal systems for financial information, the audit committee was designed to offer auditors insulation from pressures by the CEO and the CFO. Second, accountants are required to attest publicly to the adequacy of the company's internal systems for financial information under section 404, and thus they must disclose to the market any material weaknesses they identify. By forcing auditors to put their reputation on the line through public attestation and public disclosure, Sarbanes-Oxley sought to boost auditors' negotiating position vis-a-vis management, while also providing additional information to investors.

While Sarbanes-Oxley's stricter due diligence obligations underlined the monitoring function of gatekeepers, they failed to change auditors' calculations when determining whether to turn against a client. Accusing a company's management of tinkering with its financial statements remains a bold move, one that auditors are unlikely to make without strong evidence supporting their allegations. For all their credentials of independence, audit committees are likely to be reluctant to start a fight with management officials unless they can substantiate their concerns. Thus, a significant amount of evidence will be necessary before such steps can be taken. Relying exclusively on their own investigating powers, and

having to go through company officials in order to collect their data, gatekeepers may not be able to surreptitiously collect the necessary evidence.

Similarly, empirical studies of material weakness disclosures under Section 404 suggest that the strategy has only partially worked, and may even have backfired under certain circumstances. On the one hand, firms with auditor-disclosed material weaknesses suffer higher costs of capital[62] and tend to remedy the problem after a year.[63] On the other hand, two thirds of all public companies do not disclose a material weakness until after an earnings restatement.[64] Thus, the disclosure does not operate preemptively, as Sarbanes-Oxley intended. Not surprisingly, firms and auditors that do not have material weaknesses disclosed are less likely to face litigation, possibly because they can plausibly deny they were aware of the weakness, and thus avoid liability.[65] Effectively, the lack of disclosure protects auditors and clients from liability, and probably gains auditors their clients' loyalty.

2. Dodd-Frank: Empowering Whistleblowers

Since detecting financial fraud is notoriously hard, enforcement authorities have an easier job when someone with privileged access to information alerts them about ongoing fraud. People who "blow the whistle" on corporate fraud are often employees of the perpetrator, but can also be its business partners or subcontractors, or even journalists who collected evidence on the company's dealings. Financial intermediaries, by virtue of their close relationship with the client, are one of the most important pools of potential informants. But acting as a whistleblower also comes with significant negative repercussions that might discourage potential informants.

---

[62] *See*, *e.g.*, Jacqueline S. Hammersley, Linda A. Myers & Catherine Shakespeare, *Market Reactions to the Disclosure of Internal Control Weaknesses and to the Characteristics of those Weaknesses Under Section 302 of the Sarbanes Oxley Act of 2002*, 13 REV. ACCT. STUD. 141, 150–62 (2008); Hollis Ashbaugh-Skaife, Daniel W. Collins, William R. Kinney, Jr. & Ryan LaFond, *The Effect of SOX Internal Control Deficiencies on Firm Risk and Cost of Equity*, 47 J. ACCT. RES. 1, 24 (2009).

[63] However, a significant 30% of all firms with disclosed material weaknesses make no effort to remedy them even after three years. *See* Karla Johnstone, Chan Li & Kathleen Hertz Rupley, *Changes in Corporate Governance Associated with the Revelation of Internal Control Material Weaknesses and Their Subsequent Remediation*, 28 CONTEMP. ACCT. RES. 331, 341 (2011).

[64] Sarah C. Rice & David P. Weber, *How Effective is Internal Control Reporting Under SOX 404? Determinants of the (Non-)Disclosure of Existing Material Weaknesses*, 50 J. ACCT. RES. 811, 826 (2012).

[65] Sarah C. Rice, David P. Weber & Biyu Wu, *Does SOX 404 Have Teeth? Consequences of the Failure to Report Existing Internal Control Weaknesses*, 90 ACCT. REV. 1169, 1174 (2015).

Once the informant uncovers the fraud and makes her intentions known to the company, to enforcement authorities, or to the public, she stands the risk of being fired.[66] Whistleblowers will find it extremely hard to find another comparable job in the industry.[67] Exposing an employer to the rest of the world is still considered morally reproachable, even if the employer's actions themselves were illegal or unfair to others. Whistleblowers are often described in derisive terms such as "rats" and "snitches."[68] For this reason, whistleblowers risk not only a significant hit at their finances, but also the loss of friendships with co-workers and the disdain of their professional and social circle.[69]

To counter the negative repercussions of whistleblowing Sarbanes-Oxley declared employer retaliation against whistleblowers a felony.[70] In practice, however, the Sarbanes-Oxley employee complaint mechanism protected employees in very limited cases.[71] Moreover, this approach does little to reverse whistleblowers' blacklisting from the very industry on which they depend professionally and have served all their lives.

Dodd-Frank took a more daring approach: to compensate for the loss of income and the destruction of future employment opportunities, it offers whistleblowers a share of the bounty. Section 922 of Dodd-Frank requires the SEC to offer to person(s) that provided information about the fraud an amount between 10% and 30% of the total monetary sanctions collected, based on the value of the information provided and the agency's policymaking priorities. The SEC established a separate Office of the Whistleblower that runs the agency's program for collecting and assessing information, estimating awards, and protecting employees from retaliation.[72] In September 2014, the SEC made headlines by awarding a record $30

---

[66] In the Dyck et al. dataset, in 82% of the cases involving an employee whistleblower whose identity became known to management, the individual employee alleged that she was fired or had to quit her job under pressure. Alexander Dyck et al., *Who Blows the Whistle on Corporate Fraud?*, 65 J. FIN. 2213, 2216 (2010).

[67] *See* Terry Morehead Dworkin, *SOX and Whistleblowing*, 105 MICH. L. REV. 1757, 1763 n.39 (2007) (citing to Beverly H. Earle & Gerald A. Madek, *The Mirage of Whistleblower Protection Under Sarbanes-Oxley*: *A Proposal for Change*, 44 AM. BUS. L.J. 1, 6 (2007)).

[68] Faqihi, *supra* note 40, at 3351.

[69] Kathleen F. Brickey, *From Enron to WorldCom and Beyond: Life and Crime After Sarbanes-Oxley*, 81 WASH. U. L.Q. 357, 365 (2003).

[70] Sarbanes-Oxley Act of 2002 § 1107, 18 U.S.C. § 1513(e) (2012) [hereinafter Section 404].

[71] According to a study of employee retaliation complaints under Sarbanes-Oxley, of the 677 cases submitted to the Secretary of Labor in the first three years, the employees won the ALJ's protection in only 6 instances. *See* Dworkin, *supra* note 67.

[72] For more information, see SEC Annual Report on the Dodd-Frank Whistleblower Program; as of the date of this Article, the 2014 Annual Report was the most recent report. *2014 Annual Report on the Dodd-Frank Whistleblower Program*, S.E.C. (Nov. 17, 2014), https://www.sec.gov/about/offices/owb/annual-report-2014.pdf.

million bounty to a single whistleblower, whose identity has remained unknown to the public.[73]

While Dodd-Frank's bounty program has met with apparent success in providing enforcement authorities with information about ongoing fraud, it also has important limitations as a model for regulating gatekeepers. To start, Dodd-Frank's rule prevents the award of bounty to professionals who stumble upon indications of fraud when conducting an audit of a company's financial statements.[74] As a result, external auditors and their advisers cannot take advantage of the bounty program. Internal control officers responsible for internal audits can be entitled to the bounty only in limited circumstances, typically when management either fails to take action to remedy the problem or actively tries to impede the investigation.[75] Another category of gatekeepers not eligible for bounty awards is persons that are already under an obligation to report violations to the SEC.[76] Over the years, the SEC has established many rules that require regulated professionals, such as broker-dealers or investment advisers, to provide various reports to the agency.[77] Excluded from the bounty program are also persons who are otherwise criminally convicted of fraud in the reported case.[78] To the extent that gatekeepers find themselves at risk of being regarded as primary participants in fraud, they will lose the right to claim bounty. Yet, determining gatekeepers' criminal exposure ex ante is not always straightforward.

That Dodd-Frank's bounty program is not intended as a measure for regulating gatekeepers is also evident in another of its key elements: it applies to individuals, but does not extend to corporations. Dodd-Frank envisages the bounty as a reward for the individual professional who does not succumb to pressures from superiors in order to help enforcement authorities. In contrast, the bounty program does not harness the corporate enforcer. There are no incentives for gatekeeper firms to set up systems that collect and assess information about their clients, to dig deeper in their due diligence efforts, or to understand clients' potentially fraudulent intentions. Even if multiple individuals within a gatekeeper firm possess a piece of the puzzle, there are no additional incentives for the corporate employer to put them together. Rather, gatekeeper firms are left to navigate the uneasy terrain between the legality of their participation in clients' transactions, and the disloyalty of referring to the authorities clients who in the end might be doing nothing illegal.

---

[73] Josh Hicks, *$30 Million Award to Tipster Underscores Banner Year for SEC Whistleblower Program*, WASH. POST, Nov. 20, 2014, at A13, *available at* www.washingtonpost.com/blogs/federal-eye/wp/2014/11/19/30-million-whistleblower-award-underscores-banner-year-for-sec-program.

[74] 1934 Act § 21F(2)(C), 15 U.S.C. § 78u-6(c)(2)(C) (2012).

[75] SEC Final Rules, 17 C.F.R §240.21F-4(2)(b)(4)(v) (2011), *available at* https://www.sec.gov/about/offices/owb/reg-21f.pdf.

[76] 1934 Act § 21F(2)(D), 15 U.S.C. § 78u-6(c)(2)(D) (2012).

[77] SEC DIVISION OF INVESTMENT MANAGEMENT, REGULATION OF INVESTMENT ADVISERS BY THE U.S. SECURITIES AND EXCHANGE COMMISSION, S.E.C. (March 2013), *available at* http://www.sec.gov/about/offices/oia/oia_investman/rplaze-042012.pdf.

[78] 1934 Act § 21F(2)(B), 15 U.S.C. § 78u-6(c)(2)(B) (2012).

3. Academic Thinkers on Gatekeeper Reform

As scandals ravaged through the financial markets in the 2000s, many scholars recognize that gatekeeper reputation alone is not sufficient to deter wrongdoing, and have debated whether and how to expand gatekeeper liability.[79] The most radical expansion of the current regime would involve holding gatekeepers strictly liable for any client wrongdoing, and would thus turn gatekeepers into insurers.[80] In theory, strict liability has major advantages: it would lead gatekeeper firms to put in place optimal monitoring systems, and would also free courts from the difficult task of trying to ascertain, ex post, what gatekeepers knew and did not know about the fraud.[81] However, a true strict liability regime would be a "draconian response"[82]; it would not only increase the price of auditor services, but would also risk entirely unraveling the market for auditor services.[83] Thus, the most far-reaching proposals currently put forth by prominent academics involve creating a strict liability regime with some limits.[84] These proposals remain controversial, with other scholars arguing instead that gatekeepers should only be held liable for what they knew[85] or should have known.[86]

---

[79] *See, e.g.,* COFFEE, JR., CORPORATE GOVERNANCE, *supra* note 10. Frank Partnoy, *Barbarians at the Gatekeepers? A Proposal for a Modified Strict Liability Regime*, 79 WASH. U. L.Q. 491 (2001); Coffee, Jr., *Gatekeeper Failure, supra* note 10; Frank Partnoy, *Strict Liability for Gatekeepers: A Reply to Professor Coffee*, 84 B.U. L. REV. 365 (2004); John C. Coffee, Jr., *Partnoy's Complaint: A Response*, 84 B.U. L. REV. 377 (2004); *see generally* Hamdani, *supra* note 55.

[80] For a different system of third party insurance for financial statements, see Joshua Ronen, *Post-Enron Reform: Financial Statement Insurance, and GAAP Revisited*, 8 STAN. J.L. BUS. & FIN. 39 (2002).

[81] *See* STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW 9–18 (1987); Hamdani, *supra* note 55, at 83-86.

[82] Partnoy, *Strict Liability for Gatekeepers, supra* note 79, at 375.

[83] Hamdani, *supra* note 55, at 74-6.

[84] Coffee, Jr.,*Gatekeeper Failure, supra* note 10(proposing a combination of strict liability regime with a cap based on a multiple of the revenue gatekeepers received from wrongdoers); Partnoy, *Strict Liability for Gatekeepers, supra* note 79, at 375 (proposing a combination of strict liability regime with a cap based on a percentage of damages); Partnoy, *Barbarians at the Gatekeepers?, supra* note 79 (proposing the same).

[85] *See* Hamdani, *supra* note 55, at 103–104 (advocating a knowledge-based regime).

[86] Andrew F. Tuch, *Multiple Gatekeepers*, 96 VA. L. REV. 1583, 1628–31 (2010) (advocating a fault-based regime); Juan José Ganuza & Fernando Gomez, *Should We Trust the Gatekeepers? Auditors' and Lawyers' Liability for Client's Misconduct*, 27 INT'L REV. L. & ECON. 96 (2007) (proposing that under certain assumptions, the distinction between knowledge and negligence is not significant).

With the debate about how best to expand gatekeeper liability to an optimal level far from settled, recent scholarship highlights other dimensions of the gatekeeper problem that further complicate matters. Professor Lawrence Cunningham suggests that the financial industry is likely to fight any significant expansion of liability tooth and nail.[87] For this reason, he suggests that rewarding auditors for performing their gatekeeping function well rather than punishing them for gatekeeping failures, may be a more realistic way forward.[88] Professor Andrew Tuch highlights that while most of the literature is based on the simplifying assumption of a single gatekeeper, large transactions are typically reviewed by multiple gatekeepers – including a law firm, an investment bank and an accounting firm.[89] Each of these firms may have only a partial understanding of a client's business transactions, he notes, and may have incentives to "narrow the scope of its activities to reduce the likelihood that it will acquire knowledge sufficient to attract gatekeeper liability."[90] Finally, Professor Asif Hamdani distinguishes between "speaking" and "silent" gatekeepers; speaking gatekeepers make statements on which third parties rely, as in the case of accountants confirming that financial records are accurate, while "silent" gatekeepers simply fail to warn third parties.[91] Hamdani argues that market-based reputation arguments do not work in the case of silent parties, as by definition, they do not attach their name to dishonest client's activities. He also notes that while liability for silent partners in fraud could and should be expanded, it is difficult to hold a silent party civilly liable under the current securities regime.[92]

Where does this leave us? Current scholarship highlights three points. First, many scholars agree that the market-based mechanism of gatekeeper reputation does not suffice to deter financial fraud. Second, however, prominent scholars note that while significantly expanding gatekeeper liability, and turning gatekeepers into insurers, would face strong opposition from the financial industry, and might lead to a crisis in the gatekeeping professions as we know them. Third, important recent work suggests that any solutions brought forward should take into account important and heretofore unnoticed realities about the market for gatekeepers – namely that each transaction involves multiple gatekeepers, some of which are silent. The proposal that follows responds to each of these concerns.

---

[87] Cunningham, *supra* note 36 (recommending that gatekeepers be rewarded for successfully performing gatekeeping functions).

[88] *Id.*

[89] Tuch, *supra* note 86, at 1585.

[90] *Id.* at 1586.

[91] Assaf Hamdani, Silent Gatekeepers and Vicarious Liability 12 (May 2012) (on file with author), *available at* http://portal.idc.ac.il/he/schools/law/progs/legalworkshops/documents/stonerid ge%20paper%20idc.pdf.

[92] *Id.* at 8–12.

4. Gatekeepers' Potential Still Unexplored

For all the repeated attempts at reform and heated academic discussions, gatekeepers remain a resource that the current regime has not managed to fully tap. The prevailing strategy for gatekeepers seeks to entice their cooperation mostly through heavy sanctions for failing to monitor their clients. But heavy sanctions are justified when gatekeepers knowingly assisted in clients' fraud, or, in few severe cases, were negligent monitors. Not surprisingly, gatekeepers have directed their energy in clearly demarcating their knowledge or negligence, as the case may be, so that they can avoid liability. In this effort, information that does not render gatekeepers knowledgeable or negligent, but could still offer helpful tips in investigations, never reaches enforcement authorities. Worse still, gatekeepers have an incentive to suppress this information, for fear that if found out, it might be considered incriminatory in hindsight.

Policymakers' efforts to address this problem by opening up new channels of communication for gatekeepers and enforcement authorities have so far fallen short. Sarbanes-Oxley tried to get external auditors to entrust their concerns either to independent directors or even to the market itself. Not surprisingly, neither of these new outputs has yielded much. Before becoming certain that their clients are violating the law, gatekeepers are unlikely to turn openly and publicly against them, especially if voicing concerns can later be used in a lawsuit against the gatekeeper itself. Dodd-Frank's whistleblower rules offer a valuable framework for disillusioned employees and other insiders, but do not fit corporations dedicated at monitoring.

Still, in a financial system that grows ever more vast, complicated, and interconnected, our regulators cannot afford to ignore the indications of fraud that gatekeepers are bound to come across. We need a framework that allows gatekeepers to share this information, while also protecting them from the negative consequences they might face down the line. If they fail to do so, their liability should be tied to the severity of their particular failure, rather than the full extent of the underlying fraud. The following section proposes such a system.

III. Collaborative Gatekeepers: Elements of a New Paradigm

The model proposed here seeks to motivate gatekeepers to share client information that has so far remained untapped in enforcement efforts. While interacting with a client hiding misconduct, the gatekeeper may come across some indications that raise suspicions, but fall far short of confirming problems. But since these indications might prove extremely useful for enforcement authorities, our proposal requires gatekeepers to report suspicions to regulators without informing clients. In return for submitting their suspicions, gatekeepers gain immunity with regard to client misconduct. If they fail to submit their suspicions, gatekeepers are subject to sanctions. This framework, we argue below, can help gatekeepers

overcome conflicts of interest because it incentivizes them to report as soon as they realize something is amiss, before investing even greater efforts in building client relationships. Anonymity shields gatekeepers from clients' objections, and immunity tempers fears of self-incrimination. Rather than barricading themselves behind alleged unawareness of client misconduct, gatekeepers can limit their exposure to client risk by collaborating with authorities.

A. Background: Collecting Client Information

Existing regulatory obligations already require finance professionals to obtain, or even actively collect, information about their clients. For example, client suitability rules require broker-dealers and investment advisers to understand the risk profile of their clients.[93] Accountants must attest to the adequacy of the company's internal controls, as discussed above.[94] Investment bankers must confirm the accuracy of their clients' statements at the registration stage. Moreover, financial institutions are subject to a general obligation to supervise their employees so as to ensure that they are not engaging in illegal activity, either on their own or in conjunction with clients.[95] More generally, Delaware court rulings set out general rules requiring all corporations, including gatekeepers, to set up compliance systems that monitor their employees' conduct.[96]

Gatekeepers must also make their own inquiries about their clients' needs and particularities so as to tailor their services accordingly. As gatekeepers plan client transactions, manage client accounts, or represent clients in negotiations, they come across information on clients' backgrounds, motivations, and plans. For example, a client's financial documents might have inconsistencies; a client may have abruptly fired its outside auditors right before a quarter of challenging performance; the documentation of underlying loans in a securitization might have gaps; or the timing of trades before or after corporate events might raise doubts. Under current law, this information does not reach regulators unless growing indications of misconduct risk putting the gatekeeper at fault.

---

[93] *See* THOMAS LEE HAZEN, TREATISE ON THE LAW OF SECURITIES REGULATION § 14.16 (6th ed. 2009) (outlining brokers' obligations to customers with regard to recommendations, including suitability requirements). *See also* Daniel G. Schmedlen, Jr., Note, *Broker-Dealer Sales Practice in Derivatives Transactions: A Survey and Evaluation of Suitability Requirements*, 52 WASH. & LEE L. REV. 1441 (1995).

[94] Section 404, 15 U.S.C.A. § 7262 (2012).

[95] *See* Gadinis, *supra* note 44, at 714-22 (discussing the supervision obligation using empirical data from recent SEC investigations of large and small firms for failure to supervise).

[96] *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996) (establishing that corporate directors have an affirmative duty to monitor their corporations). *See also* Hillary A. Sale, *Monitoring* Caremark's *Good Faith*, 32 DEL. J. CORP. L. 719 (2007) (celebrating the landmark *Caremark* case and its progeny).

Collaborative gatekeeping puts this information front and center. This information could point to potential illegality and offer a missing piece of the puzzle for enforcement authorities. Gatekeepers should evaluate this information and, if necessary, make additional inquiries to supplement their intelligence. Typically, these inquiries will take place at the beginning of the client relationship. Through this process, gatekeepers could assess whether their clients' conduct raises suspicions, as outlined below.

B. Key Obligation: Filing an Anonymous Suspicious Activity Report

The central part of this article's proposal is a new obligation for gatekeepers: to file a report alerting regulators to suspicious activities by their clients. *Suspicion* of misconduct is, by design, a particularly low reporting threshold, one that sets this proposal apart from gatekeeper liability provisions under the current regime.[97] Suspicions could arise when clients' rationale for pursuing a transaction has gaps, when the information they provide is inconsistent or false, or when their proclaimed strategy does not fit well with specific actions that they instruct the gatekeeper to pursue on the ground. Rather than waiting to gather evidence that fully delineates clients' illegal actions, the proposal encourages gatekeepers to come forward at a much earlier stage. Moreover, the suspicion standard incentivizes gatekeepers who only have partial information to still alert regulators about potential client misconduct. While gatekeepers have no means to collect intelligence on the remaining pieces of the puzzle, regulators can utilize their investigatory powers to extract valuable evidence.

Which client actions can give rise to a *suspicion* of illegality? Rather than relying on subjective judgments, this proposal's suspicion threshold calls for an objective, fact-based inquiry. To start, suspicions should arise when a client's conduct resembles past instances of fraud. Courts, regulators, and self-regulatory organizations have built a rich jurisprudence that determines the elements of many violation types. This wealth of materials also suggests fact patterns that tend to be connected with misconduct. For example, when a bank suddenly increases its loan granting supply, it may raise concerns that standards are falling and obligations to carefully assess borrowers' profiles are overlooked. To take a different example, intense trading around corporate events might indicate abuse of inside information.

---

[97] *See*, *e.g.*, Tellabs, Inc. v. Makor Issues & Rights, Ltd., 551 U.S. 308, 318 (2007) (noting that "to establish liability under § 10(b) and Rule 10b–5, a private plaintiff must prove that the defendant acted with scienter meaning 'a mental state embracing intent to deceive, manipulate, or defraud'" and reserving the question of whether recklessness also meets the scienter standard). *See also* 5A CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 1301.1 (3d. ed. 2011) (discussing the standards for pleading scienter after the Private Securities Litigation Reform Act of 1995). *See also* Gideon Mark, *Accounting Fraud: Pleading Scienter of Auditors Under the PSLRA*, 39 CONN. L. REV. 1097, 1097 (2007) (arguing that courts have severely limited auditor liability by setting a high scienter requirement).

In another example, reluctance to provide information about odd accounting treatments might suggest that something is amiss.

Moreover, gatekeepers might be suspicious when a client deviates abruptly and sharply from his own past conduct or departs significantly from the conduct of clients with similar profiles. For example, sudden large cash deposits might suggest money laundering; repeated trading in a stock even as its price is increasing might indicate attempts for market manipulation. Gatekeepers should seek justification for such odd patterns. By directing gatekeepers' efforts to similarities with past fraud and outlier transactions, the new gatekeeper duty can become readily administrable.

To shield gatekeepers from their clients' discontent upon a suspicions filing, the reports must remain anonymous. After all, gatekeepers are expected to actively alert authorities about their clients' conduct; one cannot imagine that this will go down well, even if no illegal activities are actually occurring. At a minimum, clients may be displeased by the administrative burden of a potential regulatory investigation. Clients might also read into the report's submission a betrayal of their trust by their closest advisors. Worse still, clients may threaten to move their business elsewhere if a report is submitted. But even if clients understood that gatekeepers have very little choice in submitting a report, and even if there is no follow-up by the authorities, the doubts, concerns, and suspicions expressed in the report's contents might still prove unnerving. To reduce acrimony between clients and gatekeepers, and protect the smooth operation of suspicious activity reporting, it is essential that reports submitted to authorities remain anonymous. Without anonymity, gatekeepers would be more likely to hold off reporting as long as possible, because they would not want to see a profitable client relationship destroyed, barring clear evidence that it could not continue.

If protecting the anonymity of reporting gatekeepers is essential for the successful operation of the model, how likely is it that the client finds out who submitted a report anyways? In many cases, no regulatory action will follow the submission of a suspicious activity report, and thus the client-gatekeeper relationship will not be disturbed. Even if an investigation begins, it is possible that a client will not be able to deduce who passed the tip to the authorities. This is because most deals involve a multitude of gatekeepers – bankers, lawyers, and accountants – assisting multiple parties, and all have a separate obligation to report. Moreover, regulators are especially likely to take action when they receive multiple reports, and thus many investigations may not point toward a single source of information. For example, regulators might investigate both the legal and the accounting aspects of a transaction at the same time, thus muddying the waters for the clients. As an additional safeguard, the contents and wording of the suspicious activity report itself will never be made available to the client, and thus clients will not be able to connect particularized facts in the report with certain gatekeepers. With these precautions, conclusively linking the investigation to a suspicious activity report, and the report to a specific gatekeeper, might prove hard for clients. That said, the risk that a client-gatekeeper relationship will be interrupted once an investigation begins cannot be excluded.

C. Sanctions for Failing to Report

Backing up gatekeepers' new obligations with sanctions is essential to alter gatekeepers' behavior. Gatekeepers who fail to report suspicions may be subject to civil penalties at the corporate level, while individual employees may be subject to monetary penalties or other disciplining sanctions. Ex ante, the threat of sanctions might prompt gatekeepers to set up effective reporting systems. Ex post, these sanctions will help regulators at trial, as much less evidence will be needed to punish gatekeepers who suspected misconduct and failed to act, than to punish gatekeepers for actively participating in fraud.

The threat of sanctions for failure to report should induce gatekeepers to submit their suspicions even in cases where gatekeeper involvement would not otherwise be punishable under other substantive law provisions. For example, gatekeepers might have suspicions about clients' misconduct, but they might not have any direct involvement themselves, and thus their actions may fall outside the scope of provisions like Rule 10b-5.[98] But under the threat of sanctions, gatekeepers now have an obligation to report even those client activities.

Elevating failure to report to an independently punishable offense also has a symbolic power, which can help bring about the cultural and institutional change in the financial industry envisaged by this proposal. Diverse audiences – clients, collaborators, even colleagues – might be displeased with having suspicions filed. To avoid clashes, gatekeepers need to convince these audiences that the report is mandatory, triggered by factual considerations over which the gatekeeper has little discretion, and must be filed even if the gatekeeper believes that the client is not engaging in misconduct. Moreover, sanctions underline that, even if a client chose to move its business elsewhere, all gatekeepers are subject to a uniform regime and would be faced with the same choices as to the filing of the report.

D. The Payoff: Immunity about Reported Actions

Most regulatory schemes seek to boost implementation through sanctions for failure to comply ex post, rather than incentives to comply ex ante. Sanctions are also an essential part of the collaborative model, as discussed in the previous section. But we also put forward an important incentive: that gatekeepers gain immunity for reported actions provided they submitted reports in good faith. This incentive, we believe, is dictated by the nature of the problem that the collaborative model seeks to address, namely to get gatekeepers to share information about their clients.

To understand why immunity is worth considering in this context, imagine that you are advising a gatekeeper who has just come across indications of client misconduct. A comprehensive report of these indications immediately creates a record of the extent of gatekeeper suspicions at the time. If it turns out that the client is indeed committing fraud, victims will ask the court to evaluate this record

[98] *See* Tellabs, *supra* note 97.

ex post. Clearly, there is a risk that the court will side with fraud victims and hold that the record meets the fault standard for gatekeeper liability, i.e. knowledge or negligence, depending on the case. Indeed, the stronger the indications of fraud, the more likely is the court to side with victims.

On the other hand, the gatekeeper faces a different outcome if she holds off from reporting her suspicions, even after fraud is revealed. Without a record of gatekeeper knowledge or negligence, the court may be more readily convinced that the gatekeeper was not at fault, and impose sanctions only for failing to identify suspicions. Still, these sanctions are likely to be less onerous than damages to fraud victims. Thus, in some cases, gatekeepers are likely to be better off by not reporting, particularly when they are uncertain about how courts will interpret their reports ex post.

The proposed immunity can alleviate this uncertainty for gatekeepers acting in good faith. With the benefit of hindsight, a court may examine the reported facts and conclude that, from an objective perspective, any professional faced with such evidence should have terminated the client relationship. Yet, if the specific gatekeeper in question acted in good faith from a subjective perspective, for example because she was still trying to sort out the client's intentions, the immunity would operate in her favor. Thus, the immunity would relieve gatekeepers from the need to tiptoe between legality and illegality, and allow them to report all relevant facts and avoid unwanted legal and regulatory adventures. Since the immunity comes into effect by law as a result of the suspicions filing, gatekeepers do not need to negotiate separate relief with enforcement authorities. Moreover, the immunity attaches to the actions reported, irrespective of the specific statutes or rules violated. For these reasons, immunity helps create a more stable and predictable regulatory environment for gatekeepers. This increased stability for gatekeepers comes at little direct cost to their business. Essentially, the proposal envisages that the gatekeeper, after reporting, can *continue* offering its services to the client, to the extent otherwise allowed by law. The relationship with the client would have to be interrupted only if the facts outlined in the report could establish that the gatekeeper is in bad faith.

The proposed immunity can help gatekeepers not only toward potential victims of clients' fraud, but also toward clients themselves. Reporting clients' suspicious activity to regulators may clash with gatekeepers' obligations toward their clients. For example, there might be professional rules mandating confidentiality or general privacy laws. By shielding gatekeepers from such causes of action, the immunity removes any remaining impediments to reporting.

While the promise of immunity may induce gatekeepers to submit a report, they still have significant leeway in deciding what facts to include in their report. Strategically minded gatekeepers might wish to provide regulators with just enough facts so as to secure the immunity benefits, while also discouraging the regulator from actually conducting further investigations. There may be doubts as to the scope of the immunity, the sincerity of the reporting gatekeeper, and the extent to which the information provided actually assisted regulators' efforts. To avoid this problem, regulators should be able to strip away the immunity from gatekeepers who withheld information from their reports intentionally or recklessly. To resolve

any disputes in accordance with principles of due process, reporting gatekeepers should have access to a hearing before regulators, as well as the ability to contest regulators' decision to strip them of the immunity in court.

E. How Can Reporting Suspicions Help Gatekeeper Professionals Overcome Conflicts of Interest?

Suspicious activity reporting pays close attention to the dynamics of the gatekeeper-client relationship, interjecting a regulatory obligation at a very early stage in the development of this relationship. At that stage, the conflicts of interest that often burden gatekeepers are less likely to have gained real strength. To start, the time and effort that gatekeepers will have invested in building the client relationship is likely to be much smaller. In some instances, suspicions may even arise right out of the client's profile, before any professional services are offered. The sooner gatekeepers take notice of suspicions and submit a report, the lower the investments they will have to make in a client relationship that might be lost if regulators decide to move forward with an action. Even on a personal level, the connections between gatekeeper professionals and clients are not as deep at this early stage, and inhibitions due to long-standing bonds are unlikely. For these reasons, suspicious activity reporting's early kick start can smooth many of the dilemmas that gatekeepers face when clients misbehave.

The high volume of suspicious activity reporting has the potential of bringing about a culture shift in the way financial professionals understand and perform their regulatory obligations. Financial executives are likely to file many reports in their career, because many fact patterns can generate suspicions of misconduct. In fact, gatekeepers will be required to file reports even when they do not believe that their client is actually violating any laws. Because the obligation to report would arise in a similar manner over any gatekeeper faced with similar client facts, reporting gatekeepers will not see themselves as standing apart from their competitors. Through these repeated filings, executives will become acquainted with the process and its mission and better understand their role as an important link in safeguarding market integrity. In this way, it is hoped, individual professionals will come to see the reports as a fulfillment of an obligation rather than the action of a fiduciary that violates their clients' trust. Similarly, the intensity of suspicions reporting can also shift the attitudes of the financial industry and the public as a whole. Instead of a rarity that needs to be excoriated, cooperation with the authorities will become a regular part of gatekeepers' continued operation.

F. How Can Reporting Suspicions Help Address Conflicts of Interest at the Corporate Level?

Suspicious activity reporting can help improve the performance of existing corporate compliance infrastructure in two ways. First, the fact-based suspicion standard provides a more workable reporting obligation because it does not require

a particularly close understanding of the specific violation in question. Second, the immunity resulting from suspicious activity reporting provides stronger incentives for corporations to build effective compliance mechanisms.

Because a client's transaction is suspicious if it simply resembles past instances of fraud, the obligation to report carries a lower evidentiary burden, thus facilitating the work of internal compliance officers. Once the suspicions threshold is met, the personal beliefs of the professional handling the client or its superiors do not really come into play. In fact, the gatekeeper could also explain in the report why it believes that its client is not actually violating the law, thus addressing any resistance that compliance officers may face in reporting clients. Turning the suspicion standard into a fact-based inquiry delinks it from the subjective disposition of individual executives, and thus reduces the pernicious impact of conflicts of interest between executives and their corporate employers. Examining whether a certain set of facts or pieces of information amounts to reportable suspicions does not require intimate knowledge of the transactions or parties involved.

Delinking reporting obligations from people with intimate knowledge of misconduct allows the gatekeeper to build a separate compliance mechanism oriented towards identifying suspicious activity and informing regulators accordingly. The gatekeeper can develop a group of specialists trained to identify problematic patterns, who will become the chief supervisors of the institution's daily activities. These specialists will combine their constantly developing knowledge of the financial system with a deep sense of mission to maintain its integrity. The fact that there is a wider circle of qualified individuals who can safeguard the company's compliance is a significant improvement over the current gatekeeper framework, which relies on the individuals with closest relationship to the potentially illicit transaction to come forward and alert regulators.

Apart from facilitating the task of internal compliance mechanisms, suspicious activity reporting also boosts the benefits that the effective operation of these mechanisms can bring to gatekeepers. In particular, the immunity associated with timely reporting can help the gatekeepers continue their services with little disturbance, even after regulators proceed against some of its executives for misconduct. Under the immunity, direct consequences – such as civil penalties, monetary awards, or damages in private lawsuits – are not likely, thus calming immediate fears about the health of the gatekeeper's finances. By pointing to its report filing, the gatekeeper can protect its reputation by showing that its compliance mechanism works effectively and has contributed to regulators' efforts. Moreover, it can argue more convincingly that the instances of misconduct within its ranks are limited to the executives already targeted by regulatory action. Thus, effective reporting and immunity can help prevent effects the collapse of the gatekeeper when some of its executives are found to have been violating the law, as was the case with Arthur Andersen following Enron's collapse.

IV. A Case Study of Collaborative Gatekeeping: The Anti-Money Laundering Regime

Part III above argues that collaborative gatekeeping holds significant promise as a theoretical proposition. However, bold policy proposals are often saddled with uncertainties. A first set of concerns centers on the feasibility of the model. Would financial institutions balk at the idea, fearful they would pay dearly for costly compliance systems, only to risk alienating clients once these were in place? And in a globalized world, where capital can easily move from one state to another, why would a country place itself at a competitive disadvantage by placing unusually strict regulations on its gatekeepers? But even if the collaborative model were adopted, a second set of questions concerns its effectiveness. Would the resulting suspicious activity reports prove informative for regulators, or would gatekeepers provide minimal information to maintain client relationships? And would regulators be able to analyze all the reports that came their way, or would they be flooded with data, unable to separate signal from noise?

To answer these questions, one could start by examining examples of collaborative gatekeeping in practice. Yet, in almost all areas of financial regulation, the conventional gatekeeper model is dominant. For all the inherent variety of policy missions in finance, from accurate disclosure in securities issuance to best execution in stock exchange transacting and to diversified investing in mutual funds, U.S. laws have entrusted the conventional gatekeeper model with serving investors and the market. This remarkable uniformity in such a foundational concept has left little room for experimentation with alternative regulatory solutions.

However, one area of financial regulation follows closely the collaborative gatekeeping model developed above: anti-money laundering laws. Anti-money laundering is the singular area where U.S. policymakers, and policymakers around the world, have opted to step off the well-trodden path, and engage in a different relationship with financial intermediaries. Therefore, there are valuable lessons in studying the anti-money laundering framework, both as it has been conceptualized in law, and as it has been implemented in practice. This Part begins our analysis of the anti-money laundering regime by studying its history, which shows how regulators and private industry came to a mutually beneficial compromise. Part V completes the analysis of this regime by exploring how it has worked in practice.

Using historical records that were recently declassified, following a 40-year embargo, we recount the origins of the money-laundering current approach in Switzerland. Switzerland, banking secrecy paradise par excellence, pioneered the modern money laundering approach following a series of bank scandals in the 1970s. The Swiss were the first to call on private banks to identify potentially suspicious transactions and alert regulators accordingly. We underline information collection as the key challenge that motivated this experimental regulatory framework. Private banks agreed to collect and report this information on two conditions: that the process for collecting information would be standardized, and that the regulatory obligation would be applicable to everyone in the industry.

This historical account of the origins of modern money-laundering laws upends conventional narratives: U.S. policymakers[99] and scholars think the U.S. pioneered modern regulatory approaches in this area. Instead, as we explore below, early US efforts, including the 1970 Bank Secrecy Act, took a very different approach. After agreeing to back the Swiss approach internationally, the U.S. adopted it domestically as well, and redesigned its regulatory infrastructure to implement it. This Part first traces the development and international spread of the Swiss approach, and then presents legal mechanisms that U.S. laws have put in place to implement it.

This historical narrative serves to illustrate the plausibility of a model that might, at first, encounter significant objections. Imposing new regulatory obligations on any industry is likely to meet powerful opposition initially. However, once a few large countries have adopted the new regulatory requirements, they have strong incentives to lobby so that all their competitors, domestically and internationally, are held to the same high standard. The pages that follow trace this upward regulatory ratchet in the adoption and spread of money-laundering laws globally. Similar processes have led to heightened regulation in many different fields – from the elimination of ozone-producing chemicals, to the strict regulation of car emissions, to uniform consumer protection, to harmonized anti-trust regimes.[100] These historical antecedents make the adoption of the collaborative model to other areas of financial regulation seem more plausible. More specifically, this historical narrative helps illustrate that it is possible to overcome industry objections, and adopt regulations requiring gatekeepers to flag suspicious activity early on.

A. The Birth of A New Model: Customer Due Diligence

"Never let a good crisis go to waste"[101] was clearly in the mind of Leo Schurmann, vice-Chairman of the Swiss National Bank ("SNB") in the 1970s. As an independent regulator overseeing the country's banking sector, SNB had been worried for a while that intricacies in the financial system could easily be used to

---

[99] *Russian Money Laundering: Hearing Before the Comm. on Banking and Fin. Servs.*, 106th Cong. 120 (1999) (statement of James A. Leach, Chairman, Comm. on Banking & Fin. Servs.), *available at* http://commdocs.house.gov/committees/bank/hba59889.000/hba59889_0f.htm.

[100] DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY (1997); Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012).

[101] Recently popularized by Rahm Emanuel, this quote is often attributed to Winston Churchill, but there is no evidence he really said it. *See* Gerald S. Seib, *In Crisis, Opportunity for Obama*, WALL ST. J. (Nov. 21, 2008), at A2, *available at* http://www.wsj.com/articles/SB122721278056345271. *See also* Fred Shapiro, *Quotes Uncovered: Who Said No Crisis Should Go to Waste?*, FREAKONOMICS (Aug. 13, 2009, 12:27 PM), http://www.freakonomics.com/2009/08/13/quotes-uncovered-who-said-no-crisis-should-go-to-waste.

hide illicit gains.[102] Generally, Swiss banking secrecy law prevented banks from sharing information about their clients with the authorities. However, the veil of secrecy was to be lifted when banks became aware that their clients were conducting illegal activities.[103] In effect, knowledge of illegality required banks to share information with the authorities and turn away clients to avoid further involvement. This duty mirrored the conventional gatekeeper model typical of U.S. regulation, and was introduced as a result of U.S. pressure through a U.S./Swiss mutual legal assistance treaty.[104] But, as Swiss central bankers very well knew, evading this duty was far too easy: banks simply had to avoid becoming aware of clients' illegalities.[105] As a result, money from doubtful sources could continue to flow into Swiss banks' coffers, fueling the central bank's concerns.

The opportunity to act upon these worries came in 1977, when a money laundering scandal hit Credit Suisse, one of the largest Swiss banks. The manager of the bank's branch in Chiasso, a Swiss-Italian border town, was assisting wealthy Italians to transfer funds out of Italy illegally. Relying on Swiss banking secrecy and using a Liechtenstein shell company, the branch official had been able to keep the scheme hidden from Credit Suisse's top management for 16 years.[106] Credit Suisse suffered a loss of 1.4 million Swiss francs (equivalent to over $2 billion in today's values). More alarmingly, the banking industry as a whole faced unprecedented public uproar. The popular press fumed against banks' practices, and politicians called for abolishing banks' privileges and creating a new federal regulator.

Schurmann, an experienced politician and law professor, seized his moment. Banks might be able to appease public anger and deflect undesirable regulatory intervention, he proposed, if they openly agreed to scrutinize their clients more closely. To lend credibility to this proposal, banks would willingly subject their information collection efforts to oversight by the Swiss National Bank. Thus, the vehicle for introducing banks' new obligations, and hopefully regaining public confidence, would be a private gentlemen's agreement, to which each bank could accede, with the Swiss National Bank as a guarantor. Internal Swiss bank

---

[102] Thomas D. Grant, *Toward a Swiss Solution for an American Problem: An Alternative Approach for Banks in the War on Drugs*, 14 ANN. REV. BANKING L. 225, 246 (1995).

[103] Swiss Federal Law on Banks and Savings Banks of Nov. 8, 1934, amended on March 18, 1994, art. 47 (Arthur Andersen et al. trans. 1996).

[104] Treaty on Mutual Assistance in Criminal Matters, May 25, 1973, United States-Switzerland, 27 U.S.T. 2019, T.I.A.S. No. 8302 (ratified by the U.S. Senate on July 10, 1976).

[105] Memorandum from the Swiss Nat'l Bank Legal Dep't to the Swiss Nat'l Bank (1977) (on file with authors).

[106] In 1977, in what is known as the Chiasso Scandal, Credit Suisse lost 1.4 billion Swiss francs when the bank's account manager lent money to shell corporations in order to help clients evade official detection of their assets. *See*, *e.g.*, *Swiss to Vote On Bank Law*, N.Y. TIMES, May 19. 1984, at 41, *available at* http://www.nytimes.com/1984/05/19/business/swiss-to-vote-on-bank-law.html; Grant, *supra* note 102, at 241.

documents outline these banks' willingness to take on additional compliance obligations as part of a concerted public relations strategy.[107]

With Schurmann in the lead, the central bank began negotiations with the Swiss Bankers' Association and the nation's major banks to hammer out the elements of this gentlemen's agreement. Minutes of the Swiss National Bank show that they knew that some of the money in Swiss banks was of "*doubtful*" origins – i.e., potential connections with crime were suspected though not positively known.[108] In the future, banks should not be able to turn a blind eye to such suspected connections. Thus, the agreement would require banks to conduct due diligence in order to ascertain the beneficial ownership of the funds. In the course of their due diligence, banks could more easily become aware of illegal connections. With awareness thus forced upon them, banks would have no choice but to cooperate with authorities.

But what if due diligence did not resolve the question fully, so that doubts about the funds still remained? At that stage, banks would be required to ask clients for further documentation, including a written and signed statement setting out the client's representations about the funds' origins.[109] Even in this scenario, the SNB suggested, banks should err on the side of caution and be allowed to provide this evidence to the authorities, without violating bank secrecy laws.[110] This was a very important victory for the regulator, because it effectively expanded the scope of banks' obligations beyond the safe haven of awareness to the unchartered territory of suspicions and doubts. In many cases, suspicions and doubts might be the best banks could do. After all, the regulator knew that banks' due diligence tools might be limited, since the individuals presenting themselves to banks would also be the ones to speak as to the origin of their funds.[111]

---

[107] Press Release, The Swiss Bankers' Agreement on Due Diligence 1-2 (June 2, 1977) (on file with authors); Letter from Swiss Bankers' Association to Swiss National Bank, (October 20, 1977) (on file with authors); Swiss National Bank Internal Communication, "Public Handling of the Swiss Bankers' Agreement", 1-4 (May 25, 1977) (on file with authors) (detailing the strategy for public relations following the publication of the Agreement); Protocol of the Advisory Board, THE SWISS BANKERS' ASSOCIATION 25-26 (June 2, 1977) (illustrating the willingness of the Swiss banking community to adopt measures which would reduce the political fallout from the Chiasso crisis) (on file with authors).

[108] Fritz Leutwiler, Minutes of SNB Bank Committee (March 31, 1977) (on file with authors) (noting that "[t]here are bank clients with noticeably doubtful, yes even criminal backgrounds, and therefore should not have been accepted, nevertheless they were accepted, and there exists related money in Swiss banks.").

[109] Agreement on the Swiss Banks' Code of Conduct with Regard to the Exercise of Due Diligence, Swiss Bankers Association-Signatory Banks, art. 6, Apr. 7, 2008, CDB 08, *available at* http://www.swissbanking.org/en/20080410-vsb-cwe.pdf.

[110] Press Report, Swiss National Bank, (1977) (on file with authors) (noting that "[i]n doubtful cases, banks should err on the side of caution . . . .").

[111] Memorandum, *supra* note 105.

Upon hearing SNB's thoughts, the banking community froze in disbelief. Political pressure, bankers were afraid, might derail the regulator into instituting vague and hard-to-satisfy legal standards.[112] Yet, bankers' initial skepticism quickly gave way to constructive engagement. The Swiss Bankers' Association believed that it would be ineffective to allow each individual bank to determine whether it had satisfied due diligence obligations. Rather, banks needed to create a uniform approach so as to ensure high-quality information gathering.[113] More specifically, standardized forms would guide bank employees in their efforts to collect information from clients, thus delineating the questions that banks should ask clients and helping bank employees evaluate clients' responses. The Swiss Bankers' Association and the SNB created a working group to produce the standard forms that would streamline the implementation of this requirement.[114]

Apart from standardization, bankers believed that another guarantee was necessary for this scheme to work: every Swiss bank should be willing to participate. Bankers justified their insistence on universal participation by arguing that, if there were a hole left in this system, however tiny, illegal money would find it and exploit it. One could imagine that they were also concerned about competition. As due diligence imposes burdens both on banks and their customers, banks that simply stay out of the scheme might immediately gain an advantage over their competitors who participate. Regardless of bankers' motivations, the regulator also wanted as broad industry participation as possible. By using their combined leverage, the SNB and the Swiss Bankers' Association managed to have practically all Swiss banks enter into the customer due diligence agreement on July 1, 1977.[115]

For all its private nature and contractual basis, the agreement also included provisions seeking to cement its implementation. Upon noticing failures to conduct due diligence, the SNB could impose significant fines on banks.[116] To resolve potential disputes, the agreement set up an arbitration tribunal.[117] Finally, signatories undertook to avoid participating in transactions designed to circumvent the agreement, or to otherwise assist clients in deceiving domestic and foreign tax and law enforcement authorities.[118]

---

[112] Internal communications between the Swiss National Bank, the Zurich Attorneys Association and the Group of Private Bankers of Geneva (on file with authors) (revealing that the two private organizations were wary that political pressure would cause the Swiss National Bank to rely on vague legal measures). *See* Letter from Zurich Att'ys Ass'n (Verein Zürichischer Rechtsanwälte Zürich) to Swiss Nat'l Bank Legal Dep't (Sept. 13, 1977) (on file with authors); Letter from Groupement des Banquiers Privés Genevois to Dr. Fritz Leutwiler, Head of Dep't of the Swiss Nat'l Bank (June 2, 1977) (on file with authors).

[113] Minutes of the Swiss Bankers Association (June 2, 1977) (on file with authors).

[114] Federal Political Department, Finance and Economics Service, Press Resease, November 1977 (on file with authors).

[115] *Id.*

[116] Agreement, *supra* note 106.

[117] *Id.* art. 14.

[118] *Id*. art. 8.

The 1977 agreement established key foundational elements of a collaborative gatekeeping model. Importantly, the agreement does not let banks off the hook if they simply fail to become aware of illegality. Rather, it requires them to assess whether there are doubts as to clients' background, and gather evidence and documentation outlining these doubts. As a result, the agreement introduces a lower threshold that banks must abide by when determining whether to grant access to the financial system: knowledge was not required; suspicions and doubts would suffice. To implement this regime, the agreement required banks to abandon their passive complacency regarding incoming clients and actively ascertain the origin of clients' wealth and the goals of clients' transactions. Thus, it introduced customer due diligence into the banking world. Through standardization, it provided banks with clear guidance about how to satisfy their new obligations, but also called for robust compliance departments in order to handle the newly required information collection efforts.

Although the 1977 agreement introduced customer due diligence as an obligation for banks, it also left a significant mismatch between banks' obligations toward clients and their relationship with law enforcement authorities. If law enforcement authorities requested information about a client in the context of an investigation, banks were free to provide it without violating bank secrecy and privacy laws, even if they only had doubts about the client. But, the 1977 agreement did not create an obligation for banks to proactively report their suspicions to the authorities. Rather, it expected that banks' newly detailed customer due diligence and recordkeeping obligations would sufficiently deter them from accepting criminals' business, since it would be far more straightforward to determine the extent of a bank's knowledge or suspicion of client misconduct. As a result, while the 1977 agreement set banks down the path of collecting information, it did not establish a mechanism for utilizing this information in order to prevent money laundering. This final step occurred when the international community embraced the Swiss due diligence obligations, as the sections below discuss.

B. A Different Model: U.S. Enacts Universal Reporting

While Switzerland was pioneering the modern-money laundering approach, contemporary U.S. regulatory efforts to fight money-laundering followed a different model. Instead of requiring banks to screen their clients closely, and ask in-depth follow up questions whenever suspicions arose, in the 1970s, American regulators' asked banks to flag every large transaction. As this approach did not bring the desired results, the U.S. adopted the conventional gatekeeping model in the 1980s.

In the early 1970s, Congress was looking for new tools to use in its fight against drugs. Drug dealers, it reasoned, had to use the financial system in order to divert profits from illegal operations into legal activities. If only authorities had a paper trail of all transactions in which customers deposit or transfer cash in significant sums, then drug dealers would have far greater difficulty laundering their

profits.[119] Creating this paper trail was a cornerstone objective of the Bank Secrecy Act of 1970.[120] The act required financial institutions to file a Currency Transaction Report ("CTR") for all deposits, withdrawals, exchanges, or transfers of currency in excess of $5,000, as well as multiple transactions conducted in the same business day by the same person if reaching that amount.[121] The reporting threshold was increased to $10,000 in 1984 and has remained unchanged ever since.[122] Besides cash, the reporting requirement was later expanded to wire transfers.[123]

The primary objective of the CTR regime is deterrence, rather than information collection. When filing a CTR, financial institutions must simply record their identity and details of the individuals appearing before them accurately, but do not have to make any further inquiries. In the CTR scheme, financial institutions are passive registers of financial flows, rather than active investigators. While Congress hoped that these records might be useful to law enforcement authorities during ongoing crime investigations, it did not really see them as jumpstarting new inquiries. Rather, Congress expected that drug dealers would be loath to have their information recorded.

Within the next decade, it became clear that the deterrent effect of CTRs would not be as prevalent as had been anticipated. After a spat of high sanctions against banks for failing to comply with their Bank Secrecy Act obligations, authorities were flooded with CTRs from around the country.[124] The vast majority of these transactions were innocent,[125] and law enforcement authorities rarely used this data for preventive reasons. Moreover, drug dealers were quick to find ways to evade being reported: they cut transactions into smaller pieces, spread them over

---

[119] Peter E. Meltzer, *Keeping Drug Money From Reaching the Wash Cycle: A Guide to the Bank Secrecy Act*, 108 BANKING L.J. 230, 231 (1991).

[120] The "Bank Secrecy Act of 1970" is the commonly-used name for The Financial Recordkeeping and Reporting in Currency and Foreign Transactions Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., and 31 U.S.C.).

[121] 31 U.S.C. 5316(d)(a) (2012) (allowing the Secretary of the Treasury to prescribe regulations to further define what amounts to cumulation of closely related events and, specifically, the term "at one time" for the purposes of that section).

[122] *See* Richard R. Cheatham & James W. Stevens, *Absent Regulatory Changes, Hispanic Immigrants Pose an Unbankable Risk*, 123 BANKING L.J. 195, 196 (2006); Wuliger v. Office of Comptroller of Currency, 394 F. Supp. 2d 1009, 1013 (N.D. Ohio 2005).

[123] Annunzio-Wylie Anti-Money Laundering Act of 1992, 18 U.S.C.A. § 1960(b)(2) (2006).

[124] John K. Villa, *A Critical View of Bank Secrecy Act Enforcement and the Money Laundering Statutes*, 37 CATH. U. L. REV. 489, 497 (1988).

[125] *Money Laundering: The Volume of Currency Transaction Reports Filed Can and Should Be Reduced: Hearing on S. 1664 Before the S. Comm. on Banking, Hous. and Urban Affairs*, 97th Cong. 1 (1994) (statement of Henry R. Wray, Director, Admin. Justice Issues), *available at* http://archive.gao.gov/t2pbat4/151052.pdf.

multiple banks and multiple dates, or used legitimate business fronts, such as restaurants, to justify cash payments.[126]

Congress responded by raising the stakes for violators through a familiar technique: criminalization. The Money Laundering Control Act of 1986[127] prohibited structuring transactions to evade reporting requirements[128] and, more lastingly, turned money laundering into a criminal offense.[129] In both cases, financial institutions would face sanctions if they assisted their customers in violating the law. This legislation introduced the conventional gatekeeper model, used throughout financial regulation in the U.S., into anti-money laundering law. Effectively, regulators relied on financial institutions as reputational intermediaries, requiring them to turn away potential money launderers, or face heavy sanctions.

Yet, courts interpreted these provisions of the Money Laundering Control Act as including a "scienter" requirement.[130] As a result, financial institutions would only be liable if they knowingly or willfully assisted their customers in money laundering. Although the defendant does not need to know the specific offense that clients are committing, mere suspicion of criminality does not satisfy scienter.[131] As money launderers devised transactions precisely in order to mask their criminal intentions, and banks were simply required to report or analyze what was presented to them, many illicit activities remained outside the scope of the law. Consistently with the traditional gatekeeper model, the financial institution's liability fell to be determined mostly *ex post*. That said, some preventive reporting requirements were also put in place, but blanket transaction reporting left authorities with too many cases to analyze fruitfully. In short, by the end of the 1980s, U.S. anti-money laundering law included both a reporting requirement for all large transactions, and many elements of the conventional gatekeeper prototype.

C. The International Community Adopts and Extends the Swiss Model: From Due Diligence to Suspicious Activity Reporting

Because financial activity – and financial fraud – cross borders easily, efforts to harmonize regulations around the world have often been proposed. But at least two models were on the table in the early 1980s: the Swiss model, requiring banks to investigate clients' suspicious activities, and the American model, requiring banks to pass on information about all large transactions. This section explores why the Swiss model was chosen as the template for global financial regulation, how global regulators extended Switzerland's efforts, and how hundreds of countries adopted the resultant regulations.

---

[126] Meltzer, *supra* note 119, at 236.
[127] 18 U.S.C.A. §§ 1956-57 (2012).
[128] 31 U.S.C.A. § 5324 (2015).
[129] 18 U.S.C. §1956(a)(1) (2012).
[130] Duncan E. Alford, *Anti-Money Laundering Regulations: A Burden on Financial Institutions*, 19 N.C. J. INT'L L. & COM. REG. 437, 458 (1994).
[131] *Id.*

Once Switzerland started requiring customer due diligence and bank recordkeeping, the international community quickly took notice, not least because the Swiss themselves were eager to advertise their banks' qualifications.[132] The Council of Europe, an international organization best known for establishing the influential European Court of Human Rights, recommended the adoption of customer due diligence principles as early as 1980.[133] In 1988, the Basel Committee on Banking Supervision, an informal meeting of G10 central bankers which issues the prominent Basel accords on capital adequacy, adopted a non-binding "Statement of Principles on the Prevention of Criminal Use of the Banking System for the Purposes of Money Laundering."[134] In its statement, the Basel Committee put its weight behind customer due diligence requirements.

These early endorsements were important in propelling customer due diligence on the international agenda as one of the key elements of a comprehensive anti-money laundering regime with global reach. To create such a regime, the G7 put together the Financial Action Task Force ("FATF"), an informal international network of officials from treasury departments and ministries of finance.[135] Over 180 countries around the world have adopted FATF's 40 Recommendations on the shape of national anti-money laundering regimes, first issued in 1990. To draft these recommendations, a group of 160 experts from around the world met in Paris for 6 months,[136] discussing alternative approaches. Having already benefitted from the support of central bankers and other international experts, customer due diligence became the prototype on the basis of which FATF framed its recommendations pertaining to the financial industry. More specifically, Recommendations 12-14 emphasized the need to identify the beneficial owners of bank accounts and to

---

[132] The Swiss Federal Department of Foreign Affairs called attention to the Agreement within international organizations as a means of indicating Swiss efforts to combat financial crime. Département Politique Fédérale de la Suisse, *Document aux représentations diplomatiques suisses* 4 (Nov. 10, 1977) (on file with authors).

[133] On June 27, 1980, the Council published Recommendation No. R (80) 10, dealing with measures to combat the transport and sheltering of illegal capital. Recommendation from the Council of Eur. Comm. of Ministers to the Council of Eur. Member States (June 27, 1980), *available at* https://www.coe.int/t/dghl/monitoring/moneyval/Instruments/Rec%2880%2910_en.pdf.

[134] BASEL COMM. ON BANKING SUPERVISION, PREVENTION OF CRIMINAL USE OF THE BANKING SYSTEM FOR THE PURPOSE OF MONEY-LAUNDERING (1988), *available at* http://www.bis.org/publ/bcbsc137.pdf.

[135] For more information on the creation of FATF and the spread of its 40 Recommendations around the world, see Stavros Gadinis, *Three Pathways to Global Standards: Private, Regulator, and Ministry Networks*, 109 AM. J. INT'L L. 1 (2015).

[136] FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING, REPORT 1990–1991, 4 (1991), http://www.fatf-gafi.org/media/fatf/documents/reports/1990%201991%20ENG.pdf.

inquire further until establishing the true identity of account owners.[137] Moreover, Recommendation 15 called for financial institutions to be vigilant toward complicated transactions with no apparent financial purpose, as they are likely to mask criminal activity.[138] These customer due diligence requirements reflect the influence of Swiss archetypes, since they require banks to move beyond passively reporting information provided by clients and toward proactively investigating the truthfulness of client representations, as well as their background.

Having thus decided in favor of a substantive due diligence obligation for financial institutions, FATF experts heavily debated what should these institutions do with the information they stand to collect. Some countries, like the U.S., which required their financial institutions to report all transactions above a certain value to authorities, pushed for a similar recommendation at a global level. Yet, most countries preferred an alternative system, where only suspicious transactions would be reported to regulators.[139] They argued that they could get similar results with a less burdensome system. Thus, Recommendations 16-18 propose that national laws permit or require financial institutions to report their suspicions to regulators, and protect them from restrictions on client confidentiality or privacy. These reports, FATF recommends, should neither be disclosed nor discussed with clients. In addition, FATF also suggested that national authorities establish databases that can easily aggregate and analyze this information.[140]

With the introduction of suspicious activity reporting through FATF's 40 Recommendations, all the building blocks of the modern anti-money laundering regime took the form they retain to this date. Most commentators saw suspicious activity reporting as a mere corollary of customer due diligence, rather than the veritable link between regulators and the financial system it was due to become. At the time, no country had implemented a suspicious activity reporting system. This would soon change, as governments and regulators turned FATF's recommendations into domestic laws. The full potential of suspicious activity reporting did not become clear until the mid-2000s, when developments in information technology assisted with analyzing large pools of information.

This section has traced the development and extension of the Swiss regulatory innovations of extensive due diligence and record keeping into the modern global system of suspicious activity reporting. This history of money-laundering provides an additional example of an upwards regulatory ratchet.[141] It shows how, once leading jurisdictions impose heightened regulatory requirements, they have incentives to help spread these around the world, to level the playing field

---

[137] FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING, THE FORTY RECOMMENDATIONS OF THE FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING 2 (1990), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf.

[138] *Id.*

[139] FINANCIAL ACTION, *supra* note 136, at 11.

[140] *See* Recommendation 24. FINANCIAL ACTION, *supra* note 137, at 4.

[141] For a discussion of upwards regulatory ratchets and other examples, see VOGEL, *supra* note 100; Bradford, *supra* note 100.

and avoid placing their firms at a competitive disadvantage. This narrative helps address a potential concern about the feasibility of the collaborative gatekeeper model –that countries will put up unyielding resistance. Instead, this history suggests that, under certain circumstances, it is possible for crises to trigger far-reaching national and even global regulatory reforms.

The following two sections discuss the incorporation of collaborative gatekeeping in U.S. anti-money laundering law. Section D discusses briefly how the U.S. Congress decided to experiment with customer due diligence and suspicious activity reporting, and how regulators implemented these congressional authorizations. Part V presents the U.S. experience with suspicious activity reports, which have come to outshine CTRs as the key method for detecting criminal links in the financial system.

D. Customer Due Diligence and Suspicious Activity Reporting in U.S. Law

As they were hard at work in negotiating the FATF Recommendations, U.S. authorities were becoming increasingly uneasy with the pitfalls of the CTR model. Not only were regulators inundated with reports of cases that had no connection to money laundering or other illegal activity, they also felt that really suspicious cases did not get reported, because clients managed to evade the reporting threshold in one way or another. This section outlines how the U.S. decided to move from the conventional gatekeeper model to the collaborative gatekeeper model in the area of money laundering, and outlines the current U.S. regulatory requirements.

Beginning in 1985, some federal banking regulators asked financial institutions to guide their investigations by pointing to particularly suspicious clients.[142] But these forms were available only to the agency soliciting them, and not to other regulators and enforcement authorities. In 1990, the Treasury asked banks to use the CTR form to report transactions that they might find suspicious. However, banks only had to tick a box for "suspicious" in their form, without a single word of explanation for the basis of their suspicions.[143] The scope of these suspicions was also very limited, as banks were under no obligation to actively investigate clients' backgrounds or motivations. To address the fragmentation of information across agencies, the Treasury Department established a specialized bureau, the Financial Crimes Enforcement Network (FinCEN), as an intelligence unit tasked with

---

[142] Press Release, U.S. Dep't of Treasury, The National Money Laundering Strategy for 2000 86 (March 2000), http://www.treasury.gov/press-center/press-releases/Documents/ml2000.pdf.

[143] U.S. GOV'T ACCOUNTABILITY OFFICE, MONEY LAUNDERING: NEEDED IMPROVEMENTS FOR REPORTING SUSPICIOUS TRANSACTIONS ARE PLANNED, REPORT TO RANKING MINORITY MEMBER, PERMANENT SUBCOMM. ON INVESTIGATIONS, SENATE COMM. ON GOVERNMENTAL AFFAIRS 3 (1995), *available at* http://gao.gov/assets/160/155076.pdf.

aggregating and analyzing reports.[144] At the same time, the Treasury lobbied Congress for a redesign of the anti-money laundering regime that would bring U.S. law in line with international standards.[145]

The desired overhaul came with the Annunzio-Wylie Anti-Money Laundering Act of 1992,[146] which triggered the shift toward collaborative gatekeeping.[147] Motivated by a foreign bank's collapse for assisting Colombian drug cartels launder money through its Miami offices,[148] the Annunzio-Wylie Act paved the way for incorporating FATF's recommendations into U.S. law. Realizing that the overly simplistic reporting system of CTRs could not capture increasingly nuanced money laundering techniques,[149] Congress introduced suspicious activity reporting as a general requirement for all U.S. financial institutions. To implement the requirement, Congress opted for a broad delegation to the Secretary of the Treasury, who was given the power to demand reports for any violation of law or regulation.[150] This sweeping authorization forms the foundation of the U.S. early reporting system, under which financial institutions alert U.S. regulators for potential money laundering and other illegal acts. The statute also prohibits filers from informing clients about their reports.[151] However, the Annunzio-Wylie Act did not define what constitutes suspicious activity, nor did it elaborate on the steps that U.S. financial institutions must take in order to comply with this obligation. The task of clarifying these concepts, which form the backbone of customer due diligence, fell on the Secretary of the Treasury.

Based on the Annunzio-Wylie authorization, the Treasury has developed a definition of suspicious activity, which applies consistently on different segments of the financial system.[152] According to Treasury rules, financial institutions must report transactions that involve funds either derived from illegal activities, or used to disguise them. Transactions designed to evade Bank Secrecy Act reporting

---

[144] U.S. GOV'T ACCOUNTABILITY OFFICE, MONEY LAUNDERING: TREASURY'S FINANCIAL CRIMES ENFORCEMENT NETWORK 5 (1991), *available at* www.gao.gov/assets/220/213999.pdf.

[145] The congressional hearings for the Annunzio-Wylie Anti-Money Laundering Act of 1992 expressly refer to Treasury's efforts to use FATF as an inspiration for the Act. *See Money Laundering Enforcement Amendments of 1991: Hearing Before Comm. on Fin. Inst. Supervision, Regulation, and Ins.*, *Comm. on Banking, Fin., and Urban Affairs*, 102nd Cong. 11-12 (1991).

[146] Alford, *supra* note 130, at 460.

[147] Eric J. Gouvin, *Bringing Out the Big Guns: The USA PATRIOT Act, Money Laundering, and the War on Terrorism*, 55 BAYLOR L. REV. 955, 967 (2003).

[148] Bank of Commerce and Credit International (BCCI) collapsed in 1991. *See* 137 CONG. REC. S9461-04 (1991) (statement of Sen. Cranson) (discussing whether UAE sales linked to international drug money laundering).

[149] Cuéllar, *supra* note 7, at 352

[150] Annunzio-Wylie Anti-Money Laundering Act of 1992 §§ 1513, 1517(b), 31 U.S.C. § 5318(g) (2014).

[151] 31 U.S.C. §5318(g)(2) (2014).

[152] *See*, *e.g.*, 12 C.F.R. § 163.180 (2011) (savings associations); 12 C.F.R. §208.62 (2015) (institutions that are members of the Federal Reserve System).

requirements, such as the $10,000 CTR threshold, are also regarded suspicious. More broadly, financial institutions must report transactions that have no business or apparent lawful purpose, or is not the sort in which the particular customer would normally be expected to engage. This definition of suspicious activity reporting places financial institutions in a fundamentally different position compared to their pre-1992 Bank Secrecy Act obligations. Rather than passively recording and reporting transactions over a certain dollar value, financial institutions are hence expected to actively seek indications of criminality or illegality. Instead of their mostly mechanistic role in the past, financial institutions now have to use their judgment in order to decide whether to report a client transaction. They also have to describe the transaction to authorities and include the reasons that give rise to their suspicions. For all these reasons, financial institutions have become active participants in the fight against money laundering and other financial crimes.

As the cornerstone of modern anti-money laundering compliance, this definition of suspicious activity reporting works in conjunction with an extensive body of other statutory rules and regulatory directives, case law, and informal guidance by regulators. Over time, subsequent legislative efforts have further enhanced the information gathering powers of the Treasury, and the obligations of financial institutions to collaborate.[153] Below, this article focuses on two elements of this regulatory apparatus that help illustrate the operation of collaborative gatekeeping: the standardization of reporting through forms, and the sanctions against financial institutions for failing to comply. The following section discusses the implementation of these legal requirements in practice.

To streamline SAR submissions, Treasury collaborated with other federal banking regulators and law enforcement authorities to develop a specific form for submitting suspicious activity reports. The form is designed to provide more comprehensive directions to filers as to the information they need to include.[154] For example, the form requires filers to pick a specific category or type with which the reported activity conforms, and to include specific identification information for filers and clients.[155] Institutions must submit a SAR within 30 days after suspicions arise.[156] SAR submissions under this regime started in April 1996. FinCEN, tasked

---

[153] Riegle Community Development and Regulatory Improvement Act of 1994, Pub. L. No. 103-325, 108 Stat. 2160, 2243 (1994) (Title IV of which is commonly known as the Money Laundering Suppression Act); Money Laundering and Financial Crimes Strategy Act of 1998, 31 U.S.C. 5340 *et seq*. (2015); International Counter-Money Laundering and Foreign Corruption Act of 2000, , US Patriot Act (2001).

[154] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 143, at 35.

[155] U.S. DEP'T OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, SUGGESTIONS FOR ADDRESSING COMMON ERRORS NOTED IN SUSPICIOUS ACTIVITY REPORTING (2007), *available at* www.fincen.gov/statutes_regs/guidance/html/SAR_Common_Errors_Web_Posting.html.

[156] 31 U.S.C. §5318(g) (2014).

with receiving and aggregating SARs, regularly issues guidance regarding how to better complete SARs.

These expansive reporting requirements gain strength through a strict sanctioning mechanism. A willful violation of the obligation to submit suspicious activity reports may entail civil penalties,[157] or even criminal penalties of up to 5 years in jail.[158] At the same time, financial institutions must maintain anti-money laundering programs that oversee compliance, train employees, and submit reports.[159] The U.S. Patriot Act, passed shortly after the 9/11 attacks, further tightened financial institutions' obligations to collect information about clients' background, business purpose, and anticipated account activity.[160] Moreover, courts have developed a "willful blindness" doctrine, under which deliberate failure to collect information amounts to willfulness to conduct money laundering.[161] This web of provisions and interpretations provides regulators with the power to enforce anti-money laundering laws closely and intently.

This Part has outlined the history of the modern anti-money-laundering regime. Using newly released archival data, we have shown how collaborative gatekeeping in the area of anti-money-laundering emerged in an unlikely country – Switzerland – and quickly spread throughout the world. Contrary to expectations, banks and other financial institutions did not fight these new regulatory requirements tooth and nail, but instead helped create them. More specifically, two critical elements of the regime, the imposition of regulatory requirements on big and small gatekeepers alike, and the standardization of reports, were introduced at the insistence of large banks. That said, we have not yet explained how this regime has worked in practice. The next Part explores this question, and shows how gatekeepers and regulators have collaborated in their efforts to implement the modern anti-money-laundering regime.

V. The Anti-Money Laundering Regime in Practice

This Part discusses the operation of the anti-money laundering regime on the ground. It helps address two critical concerns about the collaborative gatekeeper model. First, how might gatekeepers react to the requirement that clients provide early warning to regulators, and report client activity that seems suspicious? Will gatekeepers be able to separate the suspicious from the innocuous, and will they be willing to pass on this information to regulators? Second, how might regulators respond? Will they make full use of suspicious activity reports (SARs), or will they set these aside in favor of other priorities and sources of information?

As the sections below discuss, financial institutions across the U.S., representing all segments of the market and diverse lines of business, are

[157] 31 U.S.C. §5321(a)(1)&(2) (2004).
[158] 31 U.S.C. §5322(a) (2001).
[159] 31 U.S.C. §5318(h) (2014).
[160] USA PATRIOT Act § 326, 115 Stat. at 317-18 (codified at 31 U.S.C. §5318 (2014)).
[161] Cuéllar, *supra* note 7, at 344-45.

increasingly submitting SARs in recent years. This widespread embrace of suspicious activity reporting indicates a shift in the way the industry approaches money laundering: instead of withholding information out of concerns about betraying clients, financial institutions have come to view reporting as an obligation equally applicable to all. To carry out this mission, financial institutions created populous compliance departments, structured under specific regulatory guidelines and operating under regulatory supervision. They have also invested heavily in modern technology for data analysis and sharing to scout for violations, explore and analyze surrounding circumstances, and submit and review reports. This compliance infrastructure has greatly expanded gatekeepers' information processing capacity, thus boosting their chances of actually catching misconduct. But it has also changed dynamics within gatekeepers, blunting the conflict of interest between gatekeeper firms and their employees. That is, the new compliance infrastructure utilizes a broad range of employees, as well as technological infrastructure, to flag suspicious activities, rather than leaving this task to those employees who courted a particular client, and who are most likely to suffer from conflicts of interest. The industry's embrace of SARs and the related compliance infrastructure suggest that the proposed theoretical framework is not entirely impracticable.

Are these investments paying off? Does the information gathered through suspicious activity reporting have any value for enforcement authorities? The paragraphs below show that regulators believe that SARs reveal a lot, and thus devote significant time and resources in reviewing SARs. They review SARs not only to fight money laundering, but also to combat diverse types of financial crime and non-criminal fraud. Indeed, since the introduction of the SAR filing obligation, criminal cases targeting money laundering, as well as convictions, have generally increased. These developments illustrate that gatekeepers' intimate knowledge of their clients' business models, and their ability to distinguish between legitimate business proposals and potentially fraudulent ventures at an early stage, are proving valuable to regulators. They thus highlight the potential of collaborative gatekeeping as a blueprint for reforming financial regulation.

A. Volume and Quality of SAR Filings Indicates Industry Buy-In

U.S. financial institutions, though initially apprehensive about filing SARs, quickly espoused the practice with eagerness. In 1996, there were about 50,000 SARs filed with FinCEN;[162] by 2003, the SARs filed per year had risen to over 300,000.[163] Ten years later, in 2013, filed SARs had exceeded 1,600,000.[164] During

[162] U.S. DEP'T OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW: BY THE NUMBERS 1 (2004), *available at* www.fincen.gov/news_room/rp/files/sar_by_numb_03.pdf.
[163] *Id.*

this period, FinCEN has intensified its efforts to police submission of suspicious activity reports and has imposed fines some view as extraordinarily large.[165] The Department of Justice has criminally prosecuted financial institutions for anti-money laundering violations, putting some out of business.[166]

To put SARs' increase in perspective, it is worth contrasting them to Current Transaction Reports (CTRs), triggered for every transfer of over $10,000 through the financial system. The volume of CTRs has remained relatively stable over the same period, ranging from about 12 million in 1996 to over 14 million in 2011. The comparison between CTRs and SARs also reveals that financial institutions are selective about submitting a SAR. In 2011, there were over 14 million CTRs filed, compared to about 1.4 million SARs.[167] Fears that filers would simply submit a SAR for every client that crosses their institution's doorstep, and thus dilute SARs' signaling value, seem to not have materialized. Instead, it seems that the suspicions threshold pushes filers to think hard about when to alert regulators to client activity.

All segments of the market have contributed to the increase in suspicious activity reporting. Financial institutions from across the nation, big and small, in one or in multiple lines of business, are increasingly reporting their suspicions to authorities.[168] Such diversity in filers indicates that many market participants come to view reporting suspicions to regulators as their obligation. As one compliance officer stated: "There has been a cultural change in the banking industry. Before we were focusing more on the customer, now we have to focus more on compliance."[169] Indeed, finance professionals currently consider SARs as the main channel through which the U.S. government collects intelligence about money laundering.[170]

The exponential increase in SARs represents a staggering growth in the amount of tips bank regulators are receiving about money laundering. How informative are these tips for enforcement authorities? Generally, regulators treat SARs as an important source of information about financial misconduct, suggesting that many disclosures are of high quality. Reports by regulators that regularly

---

[164] U.S. DEP'T OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, SAR STATS TECHNICAL BULLETIN 1 (2014), *available at* http://www.fincen.gov/news_room/rp/files/SAR01/SAR_Stats_proof_2.pdf.

[165] David Zaring and Elena Baylis, *Sending the Bureaucracy to War*, 92 IOWA L. REV. 1359, 1414 (2007).

[166] *Id*. at 1415.

[167] U.S. DEP'T OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, ANNUAL REPORT 2011 7 (2011), *available at* http://www.fincen.gov/news_room/rp/files/annual_report_fy2011.pdf.

[168] *See, e.g.,* U.S. DEP'T OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW: BY THE NUMBERS 4 (2013) (describing filers from different segments of the market); U.S. DEP'T OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW: TRENDS, TIPS, & ISSUES 15 (2006) (discussing filings by state).

[169] NEIL KATKOV, TRENDS IN ANTI-MONEY LAUNDERING FOR CELENT 2011 5 (2011).

[170] PETER REUTER & EDWIN M. TRUMAN, CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 106 (2004).

review SARs, such as the Federal Reserve and the FDIC, have stated that they see little evidence of defensive filing, such as reports that provide only skeletal information in an effort to discharge a regulatory obligation without triggering an investigation.[171] As further discussed below, many regulators invest significant time and effort in reviewing SARs every month, which highlights the importance of SARs for their agenda.[172] As Andrew Ceresney, Director of the SEC's enforcement division, put it:

> "The SEC receives tens of thousands of tips and referrals every year from many different sources including investors, whistleblowers and SROs. But SARs coming from broker-dealers often stand out from this pack in terms of reliability because the best ones contain allegations of wrongdoing that are described clearly and comprehensively, but also concisely. This reduces the amount of research and assessment that is needed before determining whether and how to act." [173]

This does not mean that all reports are equally informative. Unfortunately, examining SAR disclosures themselves is not possible for researchers, as they are confidential by law. But regulatory institutions have described their use of SARs in a variety of annual overviews and statements. This evidence suggests that the quality of information provided through SARs varies, with some reports providing important leads for enforcement actions, and others offering little of substance.[174] FinCEN itself has stated that a number of reports do not fully sketch the reported suspicious activity, by failing to answer basic questions such as "who, what, when, were, why, and how."[175] In light of the enormous volume of reported cases, some variation in SAR quality is, perhaps, not very surprising. As FinCEN concludes, the vast majority of filed SARs are generally in line with regulatory guidance in describing activity as suspicious.[176]

An indirect way of assessing SARs' potential impact is to explore whether the increase in filings has changed the landscape for enforcing anti-money laundering laws. Indeed, U.S. data suggest that, as SAR filings have increased, so has the number of money laundering cases brought and the number of convictions won by criminal authorities.[177] To give one example, regulators report that between 2003 and 2012, depository institutions reported over 200,000 cases of suspected insider abuse, i.e.

---

[171] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 143, at 19.

[172] *See infra* Part V.E.

[173] Andrew Ceresney, *Remarks at SIFMA's 2015 Anti-Money Laundering and Financial Crimes Conference*, Feb 25, 2015, http://www.sec.gov/news/speech/022515-spchc.html.

[174] TRUMAN, *supra* note 170, at 107; *see also* Ceresney, *supra* note 173.

[175] U.S. DEP'T OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, REPORT ON OUTREACH TO DEPOSITORY INSTITUTIONS WITH ASSETS UNDER $5 BILLION 30 (2011), *available at* www.fincen.gov/news_room/rp/reports/pdf/Banks_Under_$5B_Report.pdf.

[176] *Id.*

[177] Elod Takats, *A Theory of 'Crying Wolf': The Economics of Money Laundering Enforcement* 28 (Int'l Monetary Fund Working Paper No. 07/81, 2007).

cases where bank employees used client funds for personal gain. In more than half of these cases, the executives involved were subsequently fired or suspended.[178] These connections are only tentative, because confidentiality rules prevent researchers from connecting a specific SAR to a specific conviction. That said, the fact that regulators, the only persons with the full picture, make extensive use of available SARs suggests that they find much that is useful in these reports.

B. SAR Filings Besides Money Laundering

Perhaps one of the most staggering aspects of SAR submissions is that the vast majority of reported cases do *not* involve money laundering. Indeed, only 27% of all SARs submitted to FinCEN in 2014 ended up concerning money laundering.[179] As regulators quickly realized, money laundering occurs through actions that are common in many different types of fraud. Typical activities that trigger money laundering suspicions involve transactions with no apparent economic purpose, use of multiple locations or accounts for a common goal, questionable or false documentation, counterfeit instruments, etc. All these machinations are not exclusive to money launderers, but could easily involve tax evasion, insider trading, consumer fraud, identity theft, and a host of other fraudulent and/or criminal activities.[180] As a result, SARs have opened a window into diverse criminal undercurrents in the financial system.

This extensive review of SAR information has opened regulators' eyes to problems they did not clearly see before. For example, depository institutions clearly identified elder abuse as a rising trend in financial fraud, as older Americans need to manage sizeable resources but are not as technologically savvy. A stream of SARs prompted FinCEN to conduct an extensive report and to identify practices that indicate elder abuse.[181] Moreover, SARs help regulators collect intelligence about new structures or tools in the financial system, particularly when these new tools can also facilitate misconduct. When bitcoins emerged as a successful virtual currency, SARs were crucial in providing the government with information about the bitcoin ecosystem[182] and shaping regulatory guidance.[183]

---

[178] U.S. DEP'T OF TREASURY, TRENDS, TIPS AND ISSUES, *supra* note 168, at 12-3.

[179] According to FinCEN, of the 2,413,772 activities reported in 2014 by depository institutions, only 672,136 involved money laundering. Please note that one SAR might report multiple activities. Data available in FinCEN's Quarterly Update. www.fincen.gov/news_room/rp/sar_by_number.html.

[180] *Id.*

[181] *See, e.g.,* U.S. DEP'T OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, ADVISORY TO FINANCIAL INSTITUTIONS ON FILING SUSPICIOUS ACTIVITY REPORTS REGARDING ELDER EXPLOITATION (2011), *available at* www.fincen.gov/statutes_regs/guidance/html/fin-2011-a003.html.

[182] U.S. DEP'T OF TREASURY, *supra* note 164, at 15.

[183] U.S. DEP'T OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL

SARs have also contributed a lot of granular information to well-known weaknesses of the financial system, thus aiding regulators in addressing long-standing problems with significant social consequences. Mortgage fraud, which ran rampant in the period before the 2007 collapse of the subprime market, has been targeted by FinCEN intelligence gathering efforts. As a result, the Federal Housing Agency has been able to use nearly 100,000 mortgage loan fraud SARs as the basis for subsequent action.[184] Another example of a well-known regulatory effort where SARs have made significant contributions is the fight against various forms of insider abuse, such as insider trading, breach of fiduciary duties, and other ways of using executive privileges for personal advantage.[185]

These examples of issues that SARs have helped address, outside of money laundering, are a further indication of the value of SARs as efforts to gather intelligence. At the same time, gatekeepers are not obliged to submit SARs for all types of financial fraud; these diverse SARS are submitted because money laundering sometimes intersects with other types of crimes. The extension of the suspicious activity reporting requirement seems likely to draw regulators' attention to much more misconduct.

C. Compliance Process and Technology Behind Suspicious Activity Reporting

How are SARs produced? The paragraphs that follow explain that gatekeeper firms have made major investments in personnel and technology to comply with their regulatory obligations. Technological innovations are already allowing computers to flag many suspicious transactions, so that firms need not rely solely on front-line employees who might face conflicts of interest. While these investments are sizeable, survey data suggests that firms do not find these burdens impossibly heavy. The existence of this compliance infrastructure makes the extension of the collaborative gatekeeper model to other fields more plausible.

The resources devoted by financial institutions into staffing their anti-money laundering compliance programs show the extent of private industry participation in this regulatory effort. To start with a captivating example: J.P. Morgan, the largest U.S. bank by assets,[186] has 8,000 employees working solely on anti-money laundering compliance – more than the Treasury Department and the Federal

---

CURRENCY TRADING PLATFORM (2014), *available at* http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf.

[184] U.S. DEP'T OF TREASURY, *supra* note 167, at 39.

[185] U.S. DEP'T OF TREASURY, TRENDS, TIPS AND ISSUES, *supra* note 168, at 12-3.

[186] Erik Holm, *Ranking the Biggest U.S. Banks: A New (Old) Entrant in Top 5*, Wall St. J., Dec. 10, 2014, www.blogs.wsj.com/moneybeat/2014/12/10/ranking-the-biggest-u-s-banks-a-new-old-entrant-in-top-5.

Reserve combined.[187] J.P. Morgan has about 15,000 employees working on regulatory compliance (including anti-money laundering), and 250,000 employees worldwide.[188] In large banks with multinational presence, anti-money laundering operations include one large team that concentrates information and coordinates action, and specialized officers working on the many different lines of business in the institution.[189] Big banks can have over 80 different lines of business, each with a dedicated anti-money laundering officer.[190] A medium-sized bank with over $100 billion in assets would typically have about 200 anti-money laundering officials.[191] Even the smallest banks, with up to $1 billion in assets, typically have ten or fewer anti-money laundering officials. Many of these officials started their careers as front-line employees and have a good understanding of the institution's client relationships, while others have worked in other compliance positions or in larger banks.[192]

The expanding size of anti-money laundering departments has boosted financial institutions' compliance firepower, but it is modern technology that has really revolutionized their monitoring philosophy. Financial institutions have developed software that recognizes specific transaction patterns, based on typologies sketched out on the basis of past investigations and violations.[193] This software can be enriched and adapted over time, "learning" more violations and modern techniques for money laundering. Overall, banks' newly automated systems are capable of identifying unusual patterns in transactions by sifting through multiple data points in a manner that manual laborers would find hard to imitate.

Since software typology relies on past events, it cannot catch fraudulent transaction structures that appear for the first time. To improve their alertness to money laundering novelties, financial institutions have tried an alternative approach: they use software that observes metrics of client behavior and compares them to a "peer group" of clients that are expected to behave in similar ways over time.[194] Peer groups vary by line of business, client background, geography, and other factors. In addition, most banks assess not only individual clients, but also a line of business as a whole, in terms of susceptibility to money laundering.[195]

---

[187] J.P. MORGAN, ANNUAL REPORT 2013 12 (2014), *available at* www.files.shareholder.com/downloads/ONE/329963888x0x742266/2bd13119-52d2-4d78-9d85-a433141c21ae/01-2013AR_FULL_09.pdf.

[188] Monica Langley and Dan Fitzpatrick, *Embattled J.P. Morgan Bulks Up Oversight*, WALL ST. J., Sep. 12, 2013, *available at* www.wsj.com/articles/SB10001424127887324755104579071304170686532.

[189] U.S. DEP'T OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, REPORT ON OUTREACH TO LARGE DEPOSITORY INSTITUTIONS 5 (2009), *available at* www.fincen.gov/news_room/rp/reports/pdf/Bank_Report.pdf.

[190] *Id.*

[191] KATKOV, *supra* note at 169, at 6.

[192] U.S. DEP'T OF TREASURY, *supra* note 175, at 12.

[193] U.S. DEP'T OF TREASURY, *supra* note 189, at 15.

[194] *Id*. at 14.

[195] *Id*. at 6-7.

Financial institutions' use of technological advances has been one of the primary drivers of the increase in SARs, according to finance professionals and regulators interviewed for a GAO study.[196] That said, referrals from front-line employees continue to contribute a significant amount of the cases that ultimately result into a SAR. In some banks, software-generated referrals amount to 75% of total SAR candidate cases.[197] In other banks, the picture is reversed: software contributes only 20% of their referrals.[198]

The increased use of software in anti-money laundering supervision has allowed financial institutions to outsource a significant portion of their compliance heavy lifting. This can reduce conflicts of interest significantly, by empowering many individuals besides front-line employees to report on suspicious activities. There are about 20 providers of anti-money laundering software in the world.[199] Among financial institutions, 90% find themselves running their software in house in collaboration with outside vendors, while 10% outsource their software management completely.[200] Of course, developing sophisticated software solutions and staffing populous compliance departments does not come without a cost. According to a recent survey, the aggregate global expenditure in anti-money laundering supervision in 2011 reached $5 billion per year, with $1.2 billion spent on software and $3.8 billion devoted to staff and other operational expenses.[201]

These costs are contributing to a growing trend in structuring compliance departments: increasing integration between anti-money laundering and general fraud operations. From a substantive perspective, it is becoming clear that, through anti-money laundering supervision, institutions receive alerts about other types of fraud.[202] Anti-money laundering technology can be readily used, with just a few alterations, against financial fraud more generally. Many institutions find that modern solutions applied in anti-money laundering deliver superior results compared to antiquated fraud detection systems.[203] The pressure to contain costs is particularly strong in smaller institutions, which have started to use the same staff as both anti-money laundering and anti-fraud compliance officers.[204]

Perhaps because gatekeepers directly reap some of the benefits of the early detection of client fraud, they have come to terms with these significant compliance costs. Periodic surveys of the top global banks suggest that large majorities find the anti-money-laundering regulatory burden is acceptable.[205] The significant

---

[196] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 143, at 17.
[197] U.S. DEP'T OF TREASURY, *supra* note 189, at 16-7.
[198] *Id*.
[199] KATKOV, *supra* note at 169, at 3.
[200] *Id*. at 12-13.
[201] *Id*. at 4.
[202] U.S. DEP'T OF TREASURY, *supra* note 189, at 10.
[203] KATKOV, *supra* note at 169, at 29.
[204] U.S. DEP'T OF TREASURY, *supra* note 175, at 2, 12.
[205] More specifically, KPMG surveyed a wide variety of professionals in the financial industry involved in anti-money-laundering in dozens of countries. 84% of respondents in the 2004 survey believed the regulatory burden was acceptable,

investments firms have made to combat money laundering indicate that implementing the collaborative model has proven feasible in this field. Rather than setting up compliance systems from scratch, it seems likely that firms would draw on their existing infrastructure if called on to give early warning about a broader range of fraudulent activities. In short, while the expansion of the collaborative gatekeeper model to a broad range of crimes would undoubtedly involve significant costs, experience with the AML regime suggests these might not be insurmountable.

D. Filing a SAR: Efforts for Investigation and Drafting by Front-Line Employees, Compliance Officers and Management

To assess how effectively the "suspicious activity" threshold helps filers distinguish between dubious and harmless transactions, one can look at the process for filing an SAR. Compliance officers receive information about many potentially suspicious situations, but proceed with filing in a small subset of these cases. To draw on one available example, a small financial institution conducted 439 investigations in 2009, but decided to file in only 39 cases.[206] Thus, institutions seem to put serious thought into the potential violations hidden in the situation at hand, rather than simply filing a report even in remotely suspicious cases, so as to avoid any regulatory sanctions.

Investigating a potentially suspicious transaction requires significant personnel commitment. In many institutions, the compliance officer handling the filing is a former law enforcement official or experienced investigator.[207] In other cases, it is front-line employees whose investigative efforts lay the foundation for the suspicions. In one example, a bank teller informed the anti-money laundering officer that one client's cash deposits had a strong odor of pepper, often used by drug traffickers to disorient drug-sniffing dogs.[208]

To determine whether the case merits filing, the compliance officer may present it to an oversight committee.[209] These procedures demand significant

---

93% of respondents in the 2007 survey believed the regulatory burden was either acceptable or should be increased, while 85% of respondents in the 2011 survey found the burden acceptable. This question was not repeated in the 2014 survey. While most AML professionals found the overall burden acceptable, they also desired various reforms to the system, notably more guidance and closer cooperation with regulators. See KPMG SURVEY 7 (2014), *available at* https://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3.pdf and KPMG SURVEY 9 (2011), *available at* https://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/Global-Anti-Money-Laundering-Survey-O-201109.pdf.

[206] U.S. DEP'T OF TREASURY, *supra* note 175, at 31.

[207] U.S. DEP'T OF TREASURY, *supra* note 189, at 16.

[208] U.S. DEP'T OF TREASURY, *supra* note 175, at 29.

[209] U.S. DEP'T OF TREASURY, *supra* note 189, at 6.

efforts from all employees involved. In the pepper odor case, the institution's staff spent about 160 hours collecting evidence and drafting the report.[210] To better coordinate their filing efforts, gatekeepers use case management software, which incorporates significant details, timelines, and reminders.

At the management level, compliance officers have direct links with a committee typically composed of independent board members, and can also present reports to the whole board Thus, the SAR filing process engages personnel at different levels inside the institution, who become increasingly committed to the anti-money laundering effort.

The effort that the institution puts in submitting a SAR often drives it to reevaluate its relationship with the clients involved. After a SAR is filed, financial institutions monitor the client much more closely. Some banks may inform clients that they are under monitoring, and will follow up with educational material on their anti-money laundering policies, such as brochures or letters.[211] Once a second SAR is filed, many large financial institutions are likely to close an account as a matter of practice, and consider terminating the client relationship more generally.[212] Even smaller financial institutions, for whom maintaining clientele may be more pressing, did not have difficulty deciding whether to end the relationship, apart from few cases with highly idiosyncratic facts.[213]

The procedures above suggest that, as a regulatory tool, the suspicions threshold might be striking a fine balance. On the one hand, it calls for a well-researched and justified report that gatekeepers do not seem to be undertaking lightly. On the other hand, it presents gatekeepers with a workable reporting obligation, which they can satisfy by using specialized personnel and technology.

E. Regulators in Collaboration

Collaborative gatekeeping places significant demands not only on private industry, but also on the state. Will regulators have the resources to sort through and follow up on the huge volumes of tips gatekeepers pass along? The discussion that follows explains that, to process the millions of SARs they receive as part of the anti-money laundering regime, regulators have combined conventional regulatory methods with new approaches. Significant regulator efforts to review and process SARs suggest that regulators consider the reports gatekeepers provide potentially informative.

Enforcement authorities have invested significant resources into organizing appropriate systems for analyzing the millions of AML suspicious activity reports per year. The Treasury Department has established a specialized bureau, the Financial Crimes Enforcement Network ("FinCEN"), which receives and maintains financial transaction data. FinCEN operates a single database accessible to other

---

[210] U.S. DEP'T OF TREASURY, *supra* note 175, at 29.
[211] U.S. DEP'T OF TREASURY, *supra* note 189, at 9.
[212] *Id*. at 1.
[213] U.S. DEP'T OF TREASURY, *supra* note 175, at 8.

financial regulators, criminal authorities, and other state and local bodies investigating criminals and other violators that may leave footprints on the financial system. In the first six months of 2014, FinCEN's portal received inquiries by over 350 unique agencies, including federal, state, and local authorities, self-regulatory organizations, and state attorney offices.[214] In that period, FinCEN's database received over 1 million inquiries. No other financial regulator offers comparable access to its information.

Apart from reactively opening its files to specific requests related to existing investigations, FinCEN also leads efforts to proactively scan its database in order to discover hitherto hidden misconduct. For that purpose, FinCEN has spearheaded a multi-agency task force that systematically reviews SARs to determine the viability of allegations in the report itself. Task force participants include criminal authorities such as the DEA and the FBI, regulators such as the Federal Reserve, the FDIC, and the SEC, and other agencies such as the IRS. The task force employs over 100 different SAR review teams covering different geographic areas across the country. Teams in areas with higher potential concentration of financial crime may be larger and meat more regularly than others. For example, the New York SAR review team goes over 4,000 reports per month and, after initial assessment, selects a few hundred for deeper examination.[215] According to FinCEN, these teams can cover over 180,000 SARs in a quarter. At this rate, more than 50% of all SARs submitted can get reviewed by an enforcement official.[216]

As a rulemaker, FinCEN's primary goal is to streamline the process for composing and submitting SARs. Its rules guide filers in providing information about all relevant aspects of a case in a standardized and readily researchable manner.[217] It supplements its rules with extensive guidance about handling SAR submissions. In addition, FinCEN is also providing guidance to institutions considering how to build their compliance departments so as to better satisfy their reporting obligations. For this purpose, FinCEN has collaborated with other financial regulators and created a manual specifying criteria and procedures for examining an institution's anti-money laundering compliance department.[218] First issued in 2005, the manual compiles best practices from different regulators and institutions and seeks to provide consistency in supervision.

---

[214] U.S. DEP'T OF TREASURY, *supra* note 164.

[215] Kevin Sullivan, *The Thin Green Line: The Benefits of a SAR Review Team*, ACAMS TODAY, May 29, 2012, *available at www.acamstoday.org/benefits-of-a-sar-review-team.*

[216] This calculation is based on 2014 data on submissions and reviews, and may change if SAR submission changes.

[217] FinCen allows e-filing of SARs in order to streamline submissions, enhance record keeping, and allow better and faster access to financial information. http://www.fincen.gov/forms/e-filing/Efiling_FAQs.html;
http://bsaefiling.fincen.treas.gov/Why_use_BSA_002.html.

[218] FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, BANK SECRECY ACT ANTI-MONEY LAUNDERING EXAMINATION MANUAL, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_002.htm.

To further instill compliance, regulators also followed more traditional approaches, such as bringing highly publicized enforcement actions against institutions for violating their reporting obligations. Some of these cases result from supervisory examinations that reveal weaknesses in the institutions' compliance system. Regulators will typically be satisfied with an undertaking by the board of directors that it will take remedial action, although sometimes they will require a written commitment from the institution to that effect.[219] In other cases, an institution's failure to submit required reports becomes apparent only after the underlying fraud is revealed, often to significant losses for victims. Sanctions for failure to report have become increasingly harsh in recent years.[220] FinCEN has imposed fines some view as extraordinarily large.[221] And the Department of Justice has criminally prosecuted financial institutions for money laundering violations, putting some out of business.[222]

Since the 2007/08 financial crisis, regulators and criminal enforcement authorities have used anti-money laundering law as a platform for launching some of the most far-reaching actions against some of the biggest banks, both domestic and international. Anti-money laundering violations are at the heart of four out of the eight biggest fines against banks since 2000, as tallied by the Wall Street Journal,[223] including $8.9 billion against BNP Paribas for intentionally hiding transactions with links to countries targeted by U.S. sanctions, such as Iran and Cuba; $2.6 billion against J.P. Morgan for failing to identify the Madoff fraud;[224] $2.6 billion against Credit Suisse for failing to ensure that U.S. citizens with Swiss bank accounts were not evading taxes. These cases illustrate the importance of the anti-money laundering framework as a readily available tool for instilling discipline in global banking.

Perhaps the most characteristic example involves the 2012 settlement between U.S. authorities and HSBC, which included civil penalties of $1.9 billion.[225] HSBC's U.S. subsidiary developed close links with HSBC's Mexican subsidiary and became the channel through which about $9 billion in cash and $670 in wire transfers to enter the U.S even though they could have been illegally acquired. Internal email correspondence provided clear indications that HSBC chose to turn a

---

[219] U.S. GOVERNMENT ACCOUNTABILITY OFFICE, *supra* note 143, at 18.

[220] Ben Protess & Jessica Silver-Greenberg, *JPMorgan Is Penalized $2 Billion Over Madoff*, N.Y. TIMES, Jan 8. 2014, at B1, www.dealbook.nytimes.com/2014/01/07/jpmorgan-settles-with-federal-authorities-in-madoff-case.

[221] Baylis, *supra* note 165.

[222] *Id*. at 1415.

[223] Grocer, *supra* note 5.

[224] *See infra* Part II.B.

[225] Jessica Silver-Greenberg, *HSBC Agrees to Pay Nearly $2 Billion to Settle Charges of Illegal Transfers*, N.Y. TIMES, Dec. 10, 2012, at B3, *available at* http://dealbook.nytimes.com/2012/12/11/hsbc-to-pay-record-fine-to-settle-money-laundering-charges.

blind eye to clients with potential drug cartel connections.[226] However, it was the inefficiencies in HSBC's anti-money laundering compliance that became the focus of its deferred prosecution agreement, which chastised the bank's understaffed compliance department and its decision to treat its Mexican subsidiary as low-risk.[227]

Legislation that put in place the modern anti-money-laundering regime raised two significant questions. First, would banks cooperate with the regime, reporting suspicious transactions to regulators, or would they try to turn their eyes away from potential crimes to shield their clients? Second, would regulators be able to process the information banks provided, and succeed in using it to convict money launderers? It is impossible to tell exactly how well this regime has worked, because individual suspicious activity reports remain confidential. But the high volume of suspicious activity reports' gatekeepers turn over, regulators' assessments that many of these reports are revealing, and regulators' eagerness to access SARs suggest that money-laundering legislation is no paper tiger, and might significantly dent criminal activity. Anti-money laundering efforts offer the one area where the collaborative gatekeeper model has been put into practice, with at least some success it appears. That said, is the area of money laundering highly unusual, or could this model of collaborative gatekeeping be extended to other field? The next part turns to this question.

VI. Applying the Collaborative Model In Other Areas

The collaborative gatekeeping template was implemented with some success in anti-money laundering law, growing stronger through the extensive use of information technology in recent years, as the previous two sections have chronicled. This part explores whether, and how, collaborative gatekeeping can serve as a model for other issue areas, and identifies features that facilitate its operation as well as conditions that might constrain its effectiveness.

In its simplest form, as an obligation to "know your customer" and report suspicions, the collaborative model could easily work across many different gatekeeping relationships. In various segments of the financial industry, gatekeepers already conduct some due diligence toward their clients, either because law requires it or because they need to preserve their reputation. In the context of due diligence, and their ongoing client relationships, most gatekeepers can come across potentially compromising information about their clients. One could easily imagine requiring gatekeepers to report this information. But even though the model's building blocks can be readily transplanted to other areas, they might not be as successful in catching misconduct.

---

[226] J.P. Morgan Chase Bank, *Deferred Prosecution Agreement*, Exhibit C, "Statement of Facts" (hereinafter "SOF") at ¶ 9-10, *available at* www.justice.gov/sites/default/files/opa/legacy/2012/12/11/dpa-attachment-a.pdf.

[227] Id. at ¶19, 22.

The collaborative model works best in areas where financial fraud follows well-trodden paths. Suspicions can easily arise when a gatekeeper can compare a client's conduct with the actions of other clients. To evaluate whether a client behaves a lot like past fraudsters, or simply deviates unjustifiably from current norms, a gatekeeper's point of reference is necessarily the activity of others. In turn, comparisons of transactions are easier in fields that are relatively homogenous. The more standardized the transactions a gatekeeper sees, the easier it is to identify the fraudulent ones. Moreover, relatively standardized violation types are more straightforward to investigate, as front-line gatekeeper employees can be instructed to ask specific questions or look for certain indications.

This backwards-looking perspective of the collaborative model constitutes an important limitation, both conceptual and practical. No doubt, referring to past misconduct in order to identify the future one might risk leaving innovative types of fraud off the hook. However, in many core areas of the financial system, like securities trading, standardization is quite advanced. Other areas of the financial system, like derivatives, are becoming more standardized. Moreover, as the number of financial transactions continues to grow, the data points that gatekeepers have available for their comparisons also increase. In these fields, there is a lot of currently uncollected information that could significantly improve enforcement.

In addition, the collaborative gatekeeper model works best in fields where gatekeepers control an essential component of our financial infrastructure. The payment system, which modern banks control with their deposit and wire transfer services, is a key channel for introducing new money into the financial universe. As a result, banks are well placed to collect information that might point to illegal funds. Other components of essential financial infrastructure include various stock and commodity exchanges, central depositories of securities, and central counterparties in derivatives. Most of these infrastructures allow access only to certain finance professionals under strict licensing requirements, typically imposed through regulatory supervision. Thus, these finance professionals can gather important information about types of fraud occurring through their services.

At the opposite end of the spectrum, transactions arranged privately and tailored to the needs of specific clients would be harder for gatekeepers to decode. Securitizations, collateralized debt obligations, or acquisition financing depend a lot on parties' expectations about the future, which might diverge substantially. Moreover, these transactions tend to have many moving parts, combining securities issuance, derivatives, collateralization, and corporate governance arrangements. As a result, gatekeepers in these transactions might have greater trouble identifying a party's conduct as suspicious, especially at an early stage.

Yet, even in settings of high transaction complexity, collaborative gatekeeping might prove helpful in one respect. Typically, complicated transactions tend to include multiple gatekeepers with different specializations: bankers, accountants, external auditors, and other technical experts. Some specialists get only a partial look at the transaction. Thus, although they may not be able to fully ascertain whether a transaction is fraudulent, specialists may become suspicious of how the malfunctions they identify might affect the other parts of the transaction.

These suspicions could form a basis for a report that might prove helpful for regulators, especially if multiple gatekeepers flag the same transaction.

To illustrate how these scope conditions of collaborative gatekeeping would work in the context of specific subject matters in financial regulation, the remaining sections of this Part discuss two possible extensions of the model. The first extension concerns the regulation of broker-dealers, responsible for trading in securities. Broker-dealer regulation exemplifies an area of high transaction traffic, advanced standardization, and gatekeeper control over an essential market entry-point. This extension is theoretically straightforward, and is easy to conceptualize in practice through the lens of a real life example that hit national headlines: J.P. Morgan's indictment for its role as Bernie Madoff's chief banker and broker. The second extension examines how the model might apply, after some adjustments, in a field involving varied and complicated transactions: equity offerings.

A. Collaborative Gatekeeping in Broker-Dealer Regulation

Just like banks are the essential administrators of our payment system, brokers are the key operators of our securities trading venues. Broker-dealers are the only professionals licensed to access stock exchanges, so investors need to hire them in order to trade. Moreover, brokers enjoy significant regulatory privileges, such as the ability to vouch for an investor so as to exempt transactions from registration requirements.[228] Investors seeking to buy or sell securities through these venues and private offerings typically engage a broker to act on their behalf. As a result, broker-dealers have significant information on the flow of funds in and out of key segments of the financial system. The nature of this information is very similar to information that banks collect regarding the flow of funds into the banking sector when customers deposit funds, make payments, or cash checks.

Another similarity between banks and broker-dealers is the importance of client networks. To scout the market for investor interest in the securities they trade, brokers have established multiple outposts around the country,[229] instituted online services that are increasingly popular,[230] and established branches and

---

[228] See Securities Act of 1933 § 4(2) (exempting many private placements from registration requirements); Regulation D, Securities Act of 1933, 17 C.F.R. §§ 230.501-230.508 (2008) (exempting certain primary securities offerings from federal registration) and 17 C.F.R. § 230.144A (exempting certain secondary market transactions from registration requirements).

[229] *See, e.g.,* J.P. Morgan, *supra* note 1, at 81 ((noting the presence of 5,602 branches serving over 36 million customers as of 2014).

[230] *See, e.g.,* CHARLES SCHWAB CO., ANNUAL REPORT 2014 13, 55 (2015), *available at* http://aboutschwab.com/images/uploads/inline/Schwab_2014_Annual_Report_complete.pdf (noting that over 10 million clients were served with only 325 domestic branch offices due to a large online presence).

subsidiaries across borders.[231] Moreover, brokers seek to build long-standing relationships with their clients so as to handle their securities portfolio over time. As a result, broker-dealers also have information on clients' holdings, backgrounds, and trading patterns.

Brokers' unique position at the crossroads of securities trading and their expansive client networks allow them to gather intelligence about violations for which securities' trading is the primary medium. For example, insider trading involves sales or purchases by people who possess non-public information about a security, sometimes due to their relationship with the issuer of that security.[232] Brokers possess information both about trades and about certain connections between issuers and their key executives, such as employment or marital relationships. Another example of a fraudulent scheme that relies heavily on trading is market manipulation, whereby clients seek to artificially inflate interest in their securities. Again, brokers may be able to see through clients' schemes based on the orders they are called on to execute.

Besides misconduct that centers on trading, broker-dealers' information could also help illuminate instances of fraud that happen to occur through their distribution channels. For example, brokers might buy and sell securities for private hedge funds, and thus may develop a sense of odd patterns of trading that may foreshadow the hedge fund operator's disappearance into a remote tax haven with the investors' money. In another example, a broker who is intermediating a transaction between two parties might come to realize that one party's representations might be duplicitous, and thus potentially misleading.[233]

---

[231] Michael Konczal, *A Wall Street Regulator's Race Against Time*, WASH. POST WONKBLOG, (June 22, 2013), www.washingtonpost.com/blogs/wonkblog/wp/2013/06/22/a-wall-street-regulators-race-against-time.

[232] *See* United States v. O'Hagan, 117 S. Ct. 2199, 2207 (1997) (stating that "[u]nder the "traditional" or "classical theory" of insider trading liability, § 10(b) and Rule 10b–5 are violated when a corporate insider trades in the securities of his corporation on the basis of material, nonpublic information."). See generally Yesha Yadav, *Insider Trading in Derivative Markets*, 103 GEO. L. J. 381 (2015); Donald C. Langevoort, *"Fine Distinctions" in the Contemporary Law of Insider Trading*, 2013 COLUM. BUS. L. REV. 429.

[233] *See* Press Release, SEC Charges Goldman Sachs With Fraud in Structuring and Marketing of CDO Tied to Subprime Mortgages (Apr. 16, 2010), *available at* http://www.sec.gov/news/press/2010/2010-59.htm (explaining that SEC assessed a $550 million dollar penalty, its highest ever, because "Goldman wrongly permitted a client that was betting against the mortgage market to heavily influence which mortgage securities to include in an investment portfolio, while telling other investors that the securities were selected by an independent, objective third party."). *See also* Steven M. Davidoff et al., *The SEC v. Goldman Sachs: Reputation, Trust, and Fiduciary Duties in Investment Banking*, 37 J. CORP. L. 529 (2012) (discussing this settlement).

While these indications might be readily apparent or easily available to brokers, they have little motivation to collect or use them. Under current law, broker-dealers are not under a general obligation to alert regulators about potential fraud. The general anti-fraud provisions of federal securities laws provide victims with private rights of action only if brokers were primary participants in fraud[234] and acted with scienter, i.e. intentionally or knowingly. Brokers have various obligations of a fiduciary nature toward their clients, such as to obtain the best execution for their orders,[235] to avoid trading ahead of clients,[236] and to disclose their commissions.[237] Most of these obligations aim to protect clients from brokers' own overreaching, rather than from third party fraud. Thus, information that could be useful in prosecuting fraud and other misconduct typically remains scattered and unearthed, out of the reach of regulators.

Collecting this information will probably require some additional effort both by broker-dealers and by regulators, but the institutional preconditions for launching this effort are already in place. Brokers are subject to registration with the Securities and Exchange Commission, which specifies their licensing requirements.[238] Just as federal banking regulators oversee the application of the anti-money laundering regime, the SEC could oversee the expansion of suspicious activity reporting obligations in fraud and misconduct. Broker-dealers already have in place well-staffed compliance departments and supervisory procedures, since they need to oversee employees' handling of client funds.[239] Moreover, broker-dealers are already participating in the anti-money laundering regime described above, and thus have experience with suspicious activity reporting and the infrastructure necessary to satisfy this obligation. Some broker-dealers are already using technology developed in the anti-money laundering context to keep track of

---

[234] *See* Stoneridge, *supra* note 60, at 155-6 (affirming that private plaintiffs cannot use § 10(b) of the 1934 Act to hold brokers liable for aiding and abetting fraud). *See also* Central Bank of Denver, N.A. v. First Interstate Bank of Denver, N. A., 511 U.S. 164, 191 (1994) (holding the same).

[235] FINRA Rule 2320(a) (2009). *See* FINRA Regulatory Notice 09-58, SEC Approves Amendments Regarding Best Execution and Interpositioning, 2009 WL 3320542 (SEC October 9, 2009) (applying the best execution obligation to all customer orders, including those involving interposed third parties).

[236] Investment Adviser Codes of Ethics, Investment Company Act Release No. 26, 492, 69 Fed. Reg. 41,696 (July 9, 2004) (codified at 17 C.F.R. § 275.204A-1 (2005).

[237] Rule 10b-10 (requiring brokers and dealers effecting transactions in securities to disclose commissions in writing).

[238] Article 15(d) of the 1934 Act, 15 U.S.C. §78o(d). *See also* Donald C. Langevoort & Robert B. Thompson, "Publicness" in Contemporary Securities Regulation After the JOBS Act, 101 GEO. L.J. 337, 351-54 (2013) (outlining the different gateways through which a company can become public, and the attendant requirements).

[239] *See* Gadinis, *supra* note 44, at 714-22 (discussing the supervision obligation using empirical data from recent SEC investigations of large and small firms for failure to supervise)

employee fraud. By building on their existing capabilities, brokers could easily enhance the scope of violations that are subject to greater scrutiny.

A proposal for transposing a regulatory regime from one subject matter to another might justifiably generate some hesitation, as it brings a whole industry into uncharted territory. To better understand how suspicious activity reporting might work in brokers' violations, we next turn to a case that, although brought under the anti-money laundering regime, involves fraud that would be typically associated with trading, not laundering. As discussed above, some suspicious activity that is associated with money laundering can also lead authorities to other violations. As a result, there is an overlap between the anti-money laundering regime as it currently stands, and the proposed extension of suspicious activity reporting to brokers. By analyzing a case that happens to fall within this small area of overlap, we can get a fairly good glimpse of how the suggested extension might operate in practice. Since such cases would only represent the tip of the iceberg, we can gauge whether a large mass of undetected fraud might lie beneath the surface.

In 2014, J.P. Morgan paid $2.6 billion in fines to various U.S. regulators for its role as Bernie Madoff's primary broker and bank.[240] The thrust of regulators' case relied on J.P. Morgan's failure to report any suspicions to authorities about the Madoff Ponzi scheme under the Bank Secrecy Act. J.P. Morgan, one of the largest U.S. financial institutions, holds both broker-dealer and banking licenses. Since 1986, J.P. Morgan maintained a banking relationship with various entities in the Madoff group and was in charge of the accounts through which money was directed in and out of Madoff's Ponzi scheme.[241] As a broker, J.P. Morgan intermediated on behalf of clients who sought to invest into Madoff's funds and developed derivatives based on Madoff fund returns, selling some to clients and maintaining a significant portion for itself. In the context of this relationship, J.P. Morgan came across indications that Madoff's operations were fraudulent, as the paragraphs below explain. Although J.P. Morgan's compliance systems managed to spot these indications, the investment bank failed to follow through, conduct appropriate due diligence, and file the suspicious activity reports necessary to alert regulators. Thus, the case offers a good illustration of the indications that brokers may be able to gather, the actions that they should take to pass on these tips, as well as the efforts of regulators to impose sanctions that reinforce filers' regulatory obligations.

The most important red flags that J.P. Morgan failed to evaluate properly were the consistently high abnormal returns that Madoff funds purported to generate. Individual J.P. Morgan analysts expressed surprise at these profits, which had the tendency to arise even under adverse market conditions, and concluded that they were "possibly too good to be true."[242] Due to its role as manager of Madoff's accounts, J.P. Morgan had already realized that he was engaging in transactions with no apparent or very limited economic purpose. The bank received alerts from its software about unusual third party wire activity and Treasury bond redemptions at

[240] *Supra* note 3.
[241] SOF, at ¶ 9-10.
[242] *Id.* at ¶ 29-31.

least twice.[243] Moreover, J.P. Morgan saw Madoff transferring tens of millions of dollars daily to another institution's account, only to have them return shortly thereafter.[244] None of these observations could render J.P. Morgan "aware" of the Madoff fraud, as they could also result from legal activity. Nevertheless, they were sufficient to raise suspicions of illegality, and could have led enforcement authorities to Madoff earlier.

These red flags prompted J.P. Morgan's employees to start due diligence, only to be met with Madoff's unwillingness to cooperate. Yet, these concerns were never communicated to J.P. Morgan's anti-money laundering department, and no suspicious activity reports were filed ahead of Madoff's confession and arrest. Even after Barron's, a well-respected business magazine, published an article about potential fraud at Madoff, compliance officers disregarded it, thinking that U.S. regulators would have already examined these concerns.[245] This lack of appropriate response suggests weaknesses at J.P. Morgan's compliance systems, as the bank itself has admitted. One could similarly chastise U.S. regulators for failing to take action on Madoff earlier despite urgings by the press.[246] Essentially, gatekeepers and regulators were locked into mutual inactivity, with each party waiting for the other to act, and interpreting the other's silence as tacit approval. Yet, if all relevant pieces of information were combined in a central system, perhaps this uniform inactivity would have broken down sooner.

While J.P. Morgan's U.S. operations continued their relationship with Madoff despite his unresponsiveness and lack of transparency, its U.K. subsidiary grew increasingly wary. In the U.K., J.P. Morgan's relationship with Madoff was centered on brokerage services. The bank's London team had underwritten approximately $1.14 billion in investments into Madoff's funds, including $343 million of J.P. Morgan's own money. By June 2007, the U.K. subsidiary's management called for additional due diligence on Madoff's investment strategy.[247] Although Madoff agreed to answer questions, he refused to allow full due diligence on his entities.[248] When U.K. executives tried to analyze Madoff's strategy, they also failed to explain the

---

[243] *Id.* at ¶ 21.

[244] *Id.* at ¶ 24.

[245] Erin E. Arvedlund, *Don't Ask, Don't Tell: Bernie Madoff Attracts Skeptics in 2001*, BARRON'S May 7, 2001, *available at* www.online.barrons.com/article/SB989019667829349012.html (mentioning that "[T]hree option strategists for major investment banks told Barron's they [could not] understand how Madoff churns out such numbers [using his strategy]").

[246] *Id.*

[247] The UK subsidiary had put together a Hedge Fund Underwriting Committee, who had to approve continuation of this underwriting due to its size. This committee discussed the Madoff case on June 15, 2007. Present at the meeting were a number of high-ranking executives, risk officers, and employees dealing in Madoff-related transactions. The written materials presented to the committee regarded systemic fraud as "extremely unlikely," yet the committee decided to investigate Madoff further. SOF, at ¶¶ 39–40.

[248] *Id.* at ¶ 43.

returns he was presenting. As a result, around September 2008, they decided to unwind their own positions in Madoff. A U.K. analyst explained the misgivings associated with Madoff in a lengthy memorandum on October 16, 2008, detailing Madoff's inability to confirm assets supposedly held in custody and wondering about the "'odd choice' of a small, unknown accounting firm."[249] Interestingly, the memorandum also referred to casual observations of J.P. Morgan front-line employees in their dealings with Madoff entities: they described Madoff's personnel as "defensive and almost scared of Madoff," alluding to an atmosphere where "no one dares to ask any serious questions as long as the performance is good."[250] Later in October 2008, J.P. Morgan's U.K. entities filed a suspicious activity report with the U.K. Serious Organized Crime Agency under the Proceeds of Fraud Act, reflecting the concerns outlined in the internal memorandum.[251] However, they never communicated their report to their U.S. colleagues.

J.P. Morgan's failure in reporting the Madoff fraud provides a clear illustration of how collaborative gatekeeping could work in practice. J.P. Morgan had strong suspicions, but it had also reached the end of its ability to get to the bottom of the problem, in light of Madoff's uncooperative stance. If it were required to report these suspicions and enlist the help of regulators, it could have precipitated the uncovering of Madoff's fraud and protected some investors from falling prey to his deceits. Admittedly, the SEC had received warnings about Madoff from a disgruntled former competitor, Harry Markopolos. But Markopolos had no inside information about Madoff, and many reasons to vilify him. J.P. Morgan's submissions would probably have carried a different weight in the eyes of the regulator, as they would have pitted a close collaborator and Wall Street stalwart against the secretive Ponzi-schemer. J.P. Morgan's alert would have been harder to ignore.

More generally, the Madoff example shows the type of information that brokers can collect regarding their clients. Trading flows and account movements can be a real data mine for enforcers looking for indications of fraud, providing brokers with an unparalleled overview of the financial system. The high numbers of clients and relatively homogeneous transactions that a broker supports facilitate comparisons and can readily uncover odd patterns, such as Madoff's unrealistic returns. While regulators sit behind their desks, at a distance from market developments, brokers are participants in, and entryways into, the action in the market. Their reports could be a major boost to enforcement efforts.

B. Collaborative Gatekeeping for Accountants on Equity Issuance

The collaborative model applies most straightforwardly in fields that represent a good match for its prerequisites, like broker-dealer regulation, but it also has a lot to offer in issue areas where conditions might not be as favorable. This section focuses on one such area: accountants in equity issuance. Acting as external

[249] *Id.* at ¶ 55.
[250] *Id*. at ¶ 56.
[251] *Id.* at ¶ 58.

auditors to companies issuing and selling securities to the public, accounting firms are called upon to verify the accuracy of the issuer's financial statements. This verification is a necessary precondition for a company seeking to enter the public markets, for example by listing shares on a stock exchange. Thus, accounting firms play a decisive role in determining access to a central component of our financial infrastructure. However, key features of the issuer-auditor relationship, and the regulatory regime established to govern it, render this a hard case for the collaborative model.

Compared to a broker simply executing a client's orders, the scope and intensity of accountants' services is much wider. To perform an audit of a company's financial statements, accountants must spend significant time in learning about the company, request and review extensive information, and meet repeatedly with management and key employees. Because each company has some unique features, comparisons are harder. Moreover, all the effort and resources accountants must devote toward an audit suggest that they have much to lose by reporting their clients to enforcement authorities. As accountants tend to cultivate client relationships over many years, the conflicts of interest they face may be particularly strong.

A web of regulation requires accountants, before they finalize their audit, to clarify any inhibitions they may harbor about the company's accounting, or else record them. If they fail to do so, accountants may be liable toward investors. For example, under §11 of the 1933 Securities Act, if a company's financial statements are inaccurate or misleading, investors have a claim for damages against auditors.[252] To best protect themselves from investor lawsuits, accountants who come across indications of illegality should make further inquiries and obtain clarifications from management. Fearing that management might be reluctant to provide additional information, the Private Securities Litigation Reform Act of 1995 put in place a framework designed to strengthen accountants' bargaining position against their clients. Section 10A of the Exchange Act[253] requires accountants, once they come across potentially illegal activity, to notify management (for example, the CFO) and request that remedial action be taken. If management fails to satisfy the accountants, they must submit a formal report to the board, which is also required to notify the SEC within one day. And if the board fails to notify the SEC, auditors must resign.

Sarbanes-Oxley further enhanced auditors' exposure to liability, requiring them to verify not only the accuracy of specific statements, but also the adequacy of the procedures that the company follows to gather the data necessary to draft the statements.[254] If, in examining these procedures, auditors spot weaknesses that the company refuses to address, they can publicly disclose their views to investors. Moreover, for any issues they identify with regard to management's handling of financial statements, external auditors have access to a board committee composed entirely of independent directors.

---

[252] 15 U.S.C. § 77k (1998).

[253] 15 U.S.C. 78j-1.

[254] Section 404 § 1107, 18 U.S.C. § 1513(e) (2012).

At first glance, this dense framework for the regulation of accountants, anchored in Section's 10A requirement to explore any indications of illegality, shares many features with the collaborative gatekeeping proposal we advance in this Article. However, there is a key difference. Section 10A is designed to provide the company with an opportunity to avert regulatory intervention by nipping a complaint in the bud.[255] Notifying management is the first step that accountants must take in order to clarify their suspicions, and notifying the board is the second. These steps ensure that the relationship between accountants and their clients remains as strong as ever. In reality, Section 10A mostly codifies pre-existing standards of professional conduct, and passed without any objection by the accounting industry.[256] Despite its rhetoric, Section 10A leaves accountants with the same dilemma that gatekeepers typically face. Their first option is to launch an eponymous attack on management practices, based on whatever evidence they can gather on their own, to avoid alerting their client and risk obstruction. The second option is to turn a blind eye, hoping that fraud will go undetected, or, if revealed, they will avoid liability. As we explain below, the second option might seem more appealing in many circumstances.

If accountants decide to pick a fight with management, they run the risk of losing their client and hurting their professional reputation. Whether they publicly air their disagreements with the company's financial statements, or they simply raise their concerns with independent directors, they must be able to back up their fears with some evidence. Even when accountants spot "red flags," such as mishandled transactions, mislabeled accounts, or potentially distorting diversions of funds, they need further information to determine whether these odd practices hide a real problem. On their own, accountants do not have the legal tools to dig deeper against express management wishes, or simply evasiveness. In practice, the SEC has received fewer 10A reports than hoped when the provision was passed.[257] This low reporting rate might reflect that companies actually respond to the problems pointed out by accountants. But it might also mean that it is in accountants' interest to avoid flagging problems in the first place.[258] In any case, even though accountants might have indications of potential misconduct, the current regime's notification requirements do not really encourage them to come forward.

By not acting on their suspicions, accountants are left with the second option, and may expose themselves to liability toward investors. However, they might find hope in that the relevant liability rules provide them with significant leeway. With regard to financial statements provided in a public offering of securities, §11(b)

---

[255] Gary DiBianco and Andrew M. Lawrence, *Investigation and Reporting Obligations under Section 10A of the Securities Exchange Act*, 40 Rev. Sec. Comm. Reg. 25, 31 (2007).

[256] Richard W. Painter, Lawyers' Rules, Auditors' Rules, and the Psychology of Concealment, 84 Minn. L. Rev. 1399, 1412 (2000).

[257] According to a 2003 GAO Report, a total of 29 reports had been submitted in compliance with 10A between Jan. 1, 1996 and May 15, 2003. http://www.gao.gov/assets/100/92154.pdf.

[258] John C. Coffee, The Attorney as Gatekeeper, 103 Colum. L.Rev. 1293, 1307 (2003).

allows accountants to claim a due diligence defense if they conduct a reasonable investigation into the company's practices.[259] If a company's financial statements follow a reasonable interpretation of U.S. GAAP, behind which accountants can stand in good faith, then they have satisfied their due diligence defense.[260] As far as accountants are able to show that they submitted their concerns to management, and received a somewhat satisfactory response, they should be off the hook. Accountants' risk of liability is even lower in cases where investors cannot bring a §11 claim and have to rely on Rule 10b-5, for example because the misrepresentation occurs in financial statements subsequent to a public offering. To satisfy the requirements of Rule 10b-5, plaintiffs must show that accountants provided misleading information in scienter, i.e. that they were essentially aware of the problem in the financial statements. Thus, as long as accountants can validly claim that, based on the information available to them following their inquiries, they did not have knowledge of clients' misconduct, they should be able to avoid liability.

Although such information may not prove misconduct, it could provide a promising start or a helpful boost to investigations. For example, in *In re WorldCom*, a $7 billion fraudulent scheme begun to unravel when an internal accountant discovered that $400 million held on provision for potential losses were reclassified as capital expenditures to increase the company's income.[261] Although not improper on its face, this accounting practice was unusual. As long as this information does not render accountants aware of the problem, they can continue ignoring it. Given the relatively low probability of detecting fraud, this might be a plausible strategy, but is not without its risks.

Collaborative gatekeeping offers to accountants a new option: to provide this information directly to regulators by submitting a suspicious activity report. With the anonymity of the report preserved, accountants do not risk disrupting their relationship with their clients. Clients unwilling to cooperate with external auditors have less flexibility toward regulators, who possess more extensive legal tools to extract information. If proven correct, accountants can still rely on the immunity in order to avoid liability. Thus, collaborative gatekeeping can help dislodge the strong ties between accountants and issuers, and allow the gatekeepers to overcome the conflicts of interest and alert the regulators.

VII. Conclusion

Although gatekeepers are key pillars of our regulatory framework, they often find themselves straddled between their regulatory obligations and the pressures of building client relationships in a highly competitive market. In an effort to serve

---

[259] Escott v. BarChris Construction Co., 283 F. Supp. 643, 682-83 (S.D.N.Y. 1968) (establishing the contours of the due diligence defense).

[260] Monroe v. Hughes, 31 F.3d 772, 774 (9th Cir. 1994).

[261] Susan Pulliam and Deborah Solomon, *How Three Unlikely Sleuths Exposed Fraud at WorldCom*, WALL. ST. J., Oct. 30, 2002, at A1, *available at* www.wsj.com/articles/SB1035929943494003751.

both masters at once, gatekeepers avert sanctions by making sure that they remain unaware of "red flags" indicating client misconduct. As a result, they turn a blind eye to information that could prove particularly useful in enforcement.

In this article, we have offered a novel approach out of this impasse. Our goal is not to substantially expand gatekeeper liability for clients' faults, but to entice gatekeepers to work more closely with authorities. We propose that gatekeepers report suspicions of misconduct to authorities. In return, they stand to gain immunity from actions arising out of their reports by regulators and private investors alike, provided they continue to act in good faith. But if they choose not to report promptly, then they will be subject to sanctions for failing to report, on top of any other violations they might be committing. This regime, we argue, can motivate gatekeepers to cooperate with authorities they invest significant time and effort in building a client relationship, thus fueling conflicts of interest. Moreover, the routine submission of suspicious activity reports can help change the market perception about collaborating with regulators, from a largely stigmatized decision that often costs individual professionals and firms their reputation for client loyalty, to a morally sound obligation arising from their gatekeeping function.

Rather than relying exclusively on theoretical argumentation, our collaborative gatekeeping proposal has also been tried in practice in the area of anti-money laundering law. We trace the beginnings of anti-money laundering law in Switzerland, to show that banks, rather than opposing the imposition of these rules, embraced the new regime after negotiating some compromises. We then show how most countries in the world, including the U.S., have amended and adopted the Swiss template. The implementation of this regime in the U.S. illustrates its promise to increase the flow of information from market participants to regulators. Especially with the aid of modern technology, gatekeepers and regulators were able to aggregate and review information, explore financial fraud besides money laundering, and identify areas of concern that would have otherwise gone unnoticed. We have illustrated how the collaborative model could work in two additional areas in finance, broker-dealer regulation and accounting in equity issuance.

We conclude our article by discussing some concerns that might arise in connection with the new responsibilities that regulators and private industry are to assume. Collaborative gatekeeping seems to trust regulators to read submitted reports, decide which ones are worth pursuing, investigate further, and successfully bring an enforcement action. But even if regulators did possess all the information that collaborative gatekeeping promises to bring to them, would they be able to fully take advantage of it? Regulators might lack resources and staff to pursue every lead, and might simply have other priorities. To take a famous example, the S.E.C. first learnt that something is amiss with Madoff through Harry Markopolos, a securities analyst who worked for a Madoff rival and studied Madoff's revenue stream in order to replicate it.[262] The S.E.C. even investigated Madoff in 2006 about his management of customer funds, but failed to uncover the Ponzi scheme. So, does the collaborative

[262] Gregory Zuckerman & Kara Scannell, *Madoff Misled SEC in '06, Got Off*, WALL. ST. J, Dec. 18, 2008, *available at* www.wsj.com/articles/SB122956182184616625.

model rely too heavily on government intervention, while authorities may not be up to the task?

While the collaborative model focuses on alerting regulators early, one should not underestimate the impact of the information it produces for private plaintiffs. Collaborative gatekeeping introduces a very disciplined compliance model, supported by modern technology and dedicated staff to comb through clients' operations repeatedly. This mechanism produces a detailed paper trail of staff concerns, inquiries, meetings, reports, and discussions. Without suspicious activity reporting, all these would have remained unrecorded and, in most cases, unaired. But once expressed and recorded, these documents can provide valuable ammunition to private plaintiffs seeking to establish liability. While gatekeepers would be shielded from liability under the terms of the immunity, other participants in the transaction would not have such benefits. Thus, records produced in the context of preparatory work for suspicious activity reports empower private plaintiffs as well.

Gatekeeper companies themselves might change their stance once this information is compiled. A submitted report flags a client or transaction as potentially harmful for the gatekeeper. As mentioned above, some retail banks have decided to terminate relationships with all clients that become the targets of two SARs, regardless of whether regulators decide to follow up. Thus, SARs boost the internal monitoring capacity of corporations as well, and can motivate management to look more closely into cases that might have otherwise gone unnoticed. Overall, collaborative gatekeeping's success or failure does not rest solely on the shoulders of regulators, but spurs private industry and plaintiffs into action.

But as collaborative gatekeeping seeks to transform the internal discipline and liability risk for gatekeeper firms, one might worry that it is likely to face stiff opposition from the financial industry. Clearly, intensified monitoring requires a significant investment in infrastructure and resources, which can pressure corporate profits. However, compared to other regimes of gatekeeper liability, collaborative gatekeeping has one advantage: it leaves the initiative of gatekeeping activity with the intermediaries themselves. Gatekeepers are in charge of information collection efforts and handling clients, so that they can continue to manage their relationship at every step. At the same time, gatekeepers are responsible for spotting and disciplining misbehaving employees, and even for firing failed managers, evaluating the risk of fraud at every step and reaching decisions accordingly. Moreover, gatekeepers can decide what type of compliance structure works best with their needs, which compliance staffers to hire, what they want out of their information technology, and, ultimately, which reports to submit. As a result, they are also in charge of compliance costs, and can allocate funds in a way that suits the need of their company and their business. Overall, this continuous monitoring process translates into greater certainty for gatekeeper firms, because it offers them a way to manage suspicious clients before these clients grow into an inextricable problem.

Gatekeepers' autonomy to set up a monitoring system that fits the needs of their firm and area of activity, which our proposal offers, is also one of the key advantages that advocates of strict liability typically underline. At the same time,

our proposal is unlikely to distort the gatekeeper business model to the extent that strict liability proposals might. Even proponents of strict liability recognize the possibility of overdeterrence and market distortions arising from the substantially higher fees that gatekeepers will be forced to charge. Instead, the collaborative gatekeeping model simply adds a reporting obligation, whose anonymous character and standardized application over the entire industry seek to minimize any negative market fallout. For these reasons, collaborative gatekeeping is far more palatable politically to the industry, while also bringing about important changes put forward by other reform proposals.

Calls for increasing gatekeeper liability persist loudly many years after the financial crisis, as bankers and other finance professionals continue to attract the ire of policymakers and the wider public. But, perversely, increased gatekeeper liability ties the fortunes of gatekeepers with the fate of their misbehaving clients, at times pushing gatekeepers to ally with fraudsters rather then working against them. Instead, our goal should be to offer gatekeepers a way to disassociate themselves from their clients, provided they contribute enough to the enforcement process. To reform the conventional gatekeeper model in this direction, we need to think out of the box. In this article, we started from the same premise that gatekeepers' critics start, namely that gatekeepers do not always act to prevent potential fraud, even though they have reasons to suspect that it is about to happen or is already under way. But rather than simply punishing gatekeepers for their failings, we reconceptualized this problem as one of information retention and dissemination, and proposed ways to help gatekeepers share their information. Gatekeepers are often eyewitnesses when financial fraud happens, eyewitnesses with valuable, if partial, information. Rather than alienating them, we are better off bringing them to our side.