ICLG

The International Comparative Legal Guide to:

Anti-Money Laundering 2019

2nd Edition

A practical cross-border insight into anti-money laundering law

Published by Global Legal Group, with contributions from:

Allen & Gledhill LLP
Allen & Gledhill (Myanmar) Co., Ltd.
Allen & Overy LLP
AlShamsi Lawyers & Legal Consultants
Anagnostopoulos
Blake, Cassels & Graydon LLP
BONIFASSI Avocats
Castillo Laman Tan Pantaleon & San Jose
City Legal
Debevoise & Plimpton LLP
DQ Advocates Limited
Enache Pirtea & Associates S.p.a.r.l.
Gibson, Dunn & Crutcher LLP
Herbert Smith Freehills Germany LLP
JahaeRaymakers
JMiles & Co.
Joyce Roysen Advogados
Kellerhals Carrard
King & Wood Mallesons
L&L Partners Law Offices
Linklaters LLP
Marxer & Partner Attorneys at Law
McCann FitzGerald
Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.
Nakasaki Law Firm
Nyman Gibson Miralis
Rahmat Lim & Partners
Rato, Ling, Lei & Cortés – Advogados
Rustam Kurmaev and Partners
SMM Legal Maciak Mataczyński Adwokaci Sp.k.
Vodanovic Legal
Wolf Theiss Rechtsanwälte GmbH & Co KG

glg
global legal group

global legal group

Contributing Editors
Joel M. Cohen and Stephanie Brooker, Gibson, Dunn & Crutcher LLP

Publisher
Rory Smith

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Senior Editors
Caroline Collingwood
Rachel Williams

Sub Editor
Hollie Parker

Group Consulting Editor
Alan Falach

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
May 2019

ISBN 978-1-912509-67-6
ISSN 2515-4192

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

PREFACE

We hope that you will find this second edition of *The International Comparative Legal Guide to: Anti-Money Laundering* useful and informative.

Money laundering is a persistent and very complex issue. Money laundering has been said to be the lifeblood of all financial crime, including public corruption and the financing of terrorism. Over the last 30 years, governments around the world have come to recognise the importance of strengthening enforcement and harmonising their approaches to ensure that money launderers do not take advantage of weaknesses in the anti-money laundering (AML) controls. Governments have criminalised money laundering and imposed regulatory requirements on financial institutions and other businesses to prevent and detect money laundering. The requirements are continually being refined and interpreted by government authorities. Because of the often international nature of the money laundering process, there are many cross-border issues. Financial institutions and other businesses that fail to comply with legal requirements and evolve their controls to address laundering risk can be subject to significant legal liability and reputational damage.

Gibson, Dunn & Crutcher LLP is pleased to join a group of distinguished colleagues to present several articles we hope you will find of interest on AML topics. This guide also has included chapters written by select law firms in 31 countries discussing the local AML legal and regulatory/administrative requirements and enforcement requirements. Gibson Dunn is pleased to present the chapter on the United States AML regime.

As with all ICLG guides, this guide is organised to help the reader understand the AML landscape globally and in specific countries. ICLG, the editors, and the contributors intend this guide to be a reliable first source when approaching AML requirements and considerations. We encourage you to reach out to the contributors if we can be of further assistance.

Stephanie Brooker & Joel M. Cohen

Gibson, Dunn & Crutcher LLP

Board Oversight of AML Risk: How Directors Can Navigate an Evolving World

Matthew Biben

Meryl Holt Silverman

Debevoise & Plimpton LLP

Introduction

In 2018, U.S. financial regulators and prosecutors imposed more than $1 billion in fines related to anti-money laundering ("AML") compliance failures.[1] A theme that emerges from these enforcement actions is the continued emphasis on the role of individual compliance officers, senior executives, and board members, including attempts to hold these individuals personally accountable.[2]

The focus on personal liability extends well beyond AML enforcement, forcing a spotlight onto the general oversight and compliance obligations of bank boards of directors. In particular, the penalties imposed on Wells Fargo by the Federal Reserve in February 2018 in connection with allegedly fraudulent sales practices demonstrate regulators' interest in and expectations with regard to board accountability, and have been characterised as "an attempt by the Fed to impress upon banks that their boards of directors should be vigorous, independent watchdogs – and if they fail, there will be consequences".[3]

Accordingly, the onus is on directors of financial institutions to ask the right questions to understand the bank's business and identify and prioritise the associated risks. It is critical to understand what is needed to effectively oversee and hold management accountable for complying with AML laws and regulations, as well as how to evaluate the bank's AML policies and programme. But the questions board members should ask extend well beyond financial and compliance risks to those associated with corporate culture, strategy, and operations.

This article outlines the duties of directors of financial institutions and offers a roadmap for board members trying to navigate the basic AML requirements and related key risk indicators, and their place in effective enterprise risk management, including management of strategic and operational risks that implicate a bank's business model and reputation. The considerations set forth herein have particular salience in the context of emerging – and potentially higher risk – sectors, such as cryptocurrency and marijuana, which may pose unique oversight and monitoring challenges.

Duties of Directors

In the United States, the framework for fiduciary duties and responsibilities of members of boards of directors emerges out of common law, with further definition imposed by state statutes and evolving case law.[4] The duties of care and loyalty are viewed as the traditional fiduciary duties owed by directors to the corporation, and directors are expected to carry out their corporate obligations in good faith.[5] Courts have interpreted these overarching duties as giving rise to an array of subsidiary duties that comprise director responsibilities, which can be broadly categorised as (1) the duty to exercise oversight – by remaining informed about the corporation, regularly reviewing financial statements, and inquiring into corporate affairs, for example – and (2) the duty to actively monitor performance against risk parameters as well as corporate strategy in light of attendant risks.[6]

The Delaware Court of Chancery set out the standard for directors' duty to oversee and actively monitor the corporation in *Caremark*, holding that corporate directors have an affirmative duty to establish, and exercise appropriate oversight over, some form of internal compliance activity.[7] Internal controls must be "rationally designed", though the level of detail of the control framework is a matter of business judgment.[8] In the event directors become aware of red flags, due to internal controls or through other means, they have a duty to take action.[9] *Caremark* sets a high standard for a director's breach of oversight obligations, noting that "only a sustained or systemic failure of the board to exercise oversight – such as an utter failure to attempt to assure a reasonable information and reporting system exists – will establish the lack of good faith that is a necessary condition to liability".[10]

Decisions following *Caremark* flesh out the contours of directors' fiduciary obligations. In 2012, the Delaware Court of Chancery clarified that there is a distinction between inadequate or flawed efforts and a conscious disregard by directors to meet their duty to monitor and oversee the corporation.[11]

While *Caremark* sets a demanding standard, the Wells Fargo shareholder derivative litigation offers an example of allegations involving board processes and decision-making that could result in director liability.[12] Plaintiff shareholders sued, in relevant part, the directors of Wells Fargo, alleging that they "knew or consciously disregarded that Wells Fargo employees were illicitly creating millions of deposit and credit card accounts for their customers, without those customers' knowledge or consent".[13] In particular, plaintiffs alleged that directors allowed Wells Fargo to defraud customers through "cross-selling" activities.[14] The complaint stated that the directors knew about the alleged fraudulent activity because, among other things, they were aware of letters from employees voicing concerns, complaints made through the bank's ethics hotline, lawsuits related to the fraudulent sales practices, and investigations by government agencies.[15] Plaintiffs further alleged that the defendant directors failed to ensure compliance with applicable laws, facilitated the fraudulent activity through poor oversight, and caused the bank to issue false or misleading financial statements and reports.[16]

In denying Wells Fargo's motion to dismiss and holding that the allegations met *Caremark*'s standard of conscious failure of

oversight, the court repeatedly referenced allegations that the directors had personal awareness of various red flags concerning Wells Fargo's sales practices.[17] Moreover, the court emphasised the sheer number of red flags that "collectively…support[ed] an inference that a majority of the Director Defendants consciously disregarded their fiduciary duties despite knowledge regarding widespread illegal account-creation activities, and…that there is a substantial likelihood of director oversight liability".[18] This case, while an outlier,[19] emphasises the need for directors to heed repeated indicators of a certain type of misconduct, as courts may construe the absence of a clear response as a conscious disregard to meet the duty to monitor and oversee the corporation.

Taken together, *Caremark* and subsequent cases require bank board members to stay informed about matters that could affect "judgments concerning both the corporation's compliance with law and its business performance".[20] These cases suggest that directors should put in place a formal process that routinises communications between the board and management regarding risk indicators compiled in the ordinary course and more pressing matters subject to escalation. Through this process, directors should proactively solicit and review timely and accurate information, not only about the compliance framework and business performance, but also about the broader environment and industries in which the bank is operating.

Three Lines of Defence

As a threshold matter, bank directors should familiarise themselves with the three lines of defence model, a widely adopted risk management framework. The three lines of defence model is designed to help complex organisations, such as banks, define the roles and responsibilities of front-line business personnel, practice ongoing risk management, and maintain risk management activities.[21]

The first line of defence consists of frontline employees and managers whose role is to manage risks and controls on a day-to-day basis. The second line supports senior management by establishing policies and procedures and overseeing the first-line risk management process. Meanwhile, the third line is an independent assurance function performed by internal auditors who review the corporation's risk management, controls, and governance processes at a systemic level. Internal audit generally reports independently to the board or the audit committee. The role of the board is to provide a "credible challenge" to the information and views provided by management as it carries out implementation of this risk management system.[22]

A director is expected to monitor implementation of the three lines of defence framework and be comfortable that there is sufficient information sharing and coordination among the three lines to allow for effective AML compliance risk management.

BSA/AML Risk Oversight[23]

There are various ways to keep abreast of basic AML compliance programme requirements and expectations, starting with the Federal Financial Institutions Examination Council Bank Secrecy Act ("BSA")/Anti-Money Laundering Examination Manual (the "FFIEC Manual").[24] The FFIEC Manual makes clear that the "board of directors, acting through senior management, is ultimately responsible for ensuring that the bank maintains an effective BSA/AML internal control structure, including suspicious activity monitoring and reporting. The board of directors and management should create a culture of compliance to ensure staff adherence to the bank's BSA/AML policies, procedures, and processes".[25]

Effective board oversight is supported by establishing a presentation calendar that includes regular reporting by key members of the management team, including the designated BSA compliance officer. Management is responsible for keeping the board adequately informed about risk-taking activities, which should include routine updates on key performance measurements and risk indicators that reflect the overall health of the bank's AML compliance programme. The Office of the Comptroller of the Currency ("OCC") publishes guidance that offers specific AML-related questions for directors to consider and ask based on this data.[26]

The board also has an obligation to continuously consider whether the information it receives is sufficient information upon which to make informed decisions. Directors may conclude that the board should meet with management with greater frequency, a special session of the board is necessary to collect additional information on a particular topic, an executive session of the board is needed with or without specific members of management, or engagement with management beyond the boardroom is required. Ensuring an open channel of communication with management is important, as is the ability of key officers to speak openly with the board about AML compliance issues, particularly the resources needed to address potential programme deficiencies.

In light of key issues that have been the subject of recent AML enforcement actions, directors should make sure that regular communications with management cover the following topics in relation to the bank's AML policies and procedures.

Assessing an AML Compliance Programme

Directors should first review, on a periodic basis, the bank's AML risk assessment. This risk assessment should measure inherent risk, which is the risk that an activity would pose if no controls or other mitigating factors were in place.[27] A residual risk rating should be assigned after controls are taken into account. The assessment should be candid and self-critical, especially in describing the inherent risks of doing business in a high-risk jurisdiction or providing high-risk financial services.[28] Smaller banks may not have formal written assessments, but should still engage in and document the assessment process.

Second, directors should expect regular reporting from management regarding any uncorrected supervisory issues contained in written agreements, enforcement actions, or matters requiring attention. Although criminal law enforcement agencies may identify compliance failures in the course of their investigations, most enforcement actions are brought by regulators such as the Federal Reserve or the Federal Deposit Insurance Corporation for uncorrected deficiencies previously cited during routine exams. In overseeing and holding management accountable for fixing these problems, directors should be wary of proposed solutions involving technological upgrades that might prove to be unfeasible or will take too long to implement. Board members should request regular updates from management and tracking of important milestones to ensure that deficiencies are being addressed in a timely manner.

Third, directors should know whether the bank has any uncorrected AML deficiencies identified by outside consultants. Senior managers and compliance officers at times retain outside experts to review the firm's AML compliance programme.[29] Such reviews may be triggered by unfavourable audit or exam findings, pending enforcement actions, or management's desire to proactively find and address problems. Recent AML enforcement actions have highlighted the risks to financial institutions of failing to act on

documented AML deficiencies, or withholding these third-party reports from regulators.[30] If the BSA compliance officer is new to the firm, directors should ask this individual to check the files for reports commissioned and left behind by the former BSA compliance officer.

Finally, it is important for directors to understand which employees receive AML training and what guidance is provided with respect to suspicious activity reporting. Financial institutions must ensure that appropriate personnel are trained in applicable aspects of the BSA.[31] Directors typically receive training that is tailored to their oversight role, including approving BSA/AML policies and ensuring that management is providing sufficient BSA/AML resources. But a deeper dive into questions related to who else is receiving such training and how often employees are identifying and reporting activity should provide insight into the firm's culture of compliance and whether AML compliance is viewed as a company-wide responsibility.

Identifying and Responding to Red Flags

In addition to assessing the general health of the bank's AML compliance programme, there are various topics that are key to evaluating the organisation's capacity to identify and respond to red flags. Directors should, for instance, be aware of whether the bank collects and analyses consumer and fraud complaints, and whether there are any ongoing government investigations concerning fraud by or through the bank. It is important to engage with management to understand possible fraud occurring at or through the institution, such as internet-based scams resulting in victims sending numerous but relatively small dollar transactions through the institution. In recent years, criminal prosecutors have demonstrated interest – in the form of prosecutions and large fines – for firms failing to detect, report, and halt such transactions.[32]

Directors also should inquire into the volume of suspicious activity reports ("SARs") filed through the Financial Crimes Enforcement Network ("FinCEN"), including how these numbers stand relative to the bank's peers and agency statistics. Disclosures of specific SAR filings outside of the filing institution are prohibited, but AML compliance officers are encouraged to share this information with board members. Directors should therefore expect reporting from management on key risk indicators, including, but not limited to: changes in volume with respect to transaction alerts, which identify unusual account or customer activity that may indicate financial crimes; timeline metrics, such as the average length of time between the identification of potential suspicious activity and filing of a SAR; and data that show significant spikes, drop-offs, or other changes in the volume of SAR filings. Of particular concern is under-filing of SARs, which poses greater enforcement risk than over-filing.[33] Board members should inquire about tracking of "no-SAR" decisions – *i.e.*, when potential suspicious activity is flagged but BSA staff declines to file a SAR – to make sure management is focused on evaluating and mitigating any weaknesses in organisational decision-making and record-keeping in the event of a future regulatory inquiry.

Beyond SARs and BSA requirements, compliance with sanctions regulations administered by the Office of Foreign Assets Control ("OFAC") requires financial institutions to block accounts and other property of specified countries, entities, and individuals, or prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.[34] In some instances, a bank may fail to block or reject prohibited accounts or transactions that might, upon review by the OFAC, expose the company to significant fines. Asking what transactions the institution has failed to identify and block is a good starting point in assessing the institution's customer base and risk profile.

In view of the above, directors should take a critical eye as to whether the bank has sufficient AML resources and staff. Directors must also consider whether there are Audit staff members who are competent and knowledgeable to test the AML programme. A potentially important gauge on this point is the rate of employee attrition for these departments. All institutions, large and small, at times experience significant increases in investigative caseloads that may lead to employee attrition and the loss of important institutional knowledge, and that may require devotion of additional resources. Consequently, directors should work with management to monitor staff adequacy based on caseload and average throughput per investigator. Directors should also endeavour to find out if the bank has a backlog with respect to compliance alerts or cases in order to protect the institution from potential supervisory action.

The Intersection of AML & Enterprise Risk Management

Opportunities presented by emerging industries such as cryptocurrency and marijuana demonstrate the intersection of AML risk and sanctions considerations with enterprise risk management, which implicates the bank's overall risk appetite and compliance culture. Board oversight mechanisms should be designed to accommodate these new opportunities, but directors should be aware that choices regarding engagement with these sectors may have a significant effect on the bank's business model, capabilities, resources, and reputation. As a result, risk management requires not only clear-eyed attention to the legal and regulatory challenges, but also the operational competence and agility to capitalise on new developments.

Cryptocurrency

As evidenced by JPMorgan's announcement of JPM Coin in February 2019, banks are starting to move beyond exploration of blockchain and arguably into cryptocurrency.[35] This move follows rapid growth and increased investment in the cryptocurrency and initial coin offering markets and takes place against a backdrop of heightened regulatory scrutiny.

FinCEN has made clear since 2013 that all sellers of cryptocurrency tokens, including in the context of an initial coin offering, are money services businesses and must comply with applicable AML requirements.[36] Yet, the regulatory landscape continues to evolve as the industry develops and the various federal agencies tasked with enforcement, including the Securities and Exchange Commission, the Commodity Future Trading Commission, and the Department of Justice, engage in closer coordination. While cryptocurrencies present many of the same risks as other financial technological innovations, peer-to-peer transaction authentication and the ability to operate independently of institutional intermediaries trained in AML compliance result in a unique set of challenges, both for financial institutions and their regulators.[37]

The same features of cryptocurrency that render it innovative – its anonymity, absence of national borders, and liquidity – result in heightened AML and sanctions risks of which banks and their boards of directors should be keenly aware. In particular, counterparty anonymity may pose a challenge to key elements of the bank's AML programme, including Know Your Customer and customer identification procedures. The cryptocurrency markets are also potentially exposed to risks such as facilitation of illicit

transactions and the transfer of unlawful proceeds, unknown touchpoints with criminal enterprises, as well as terrorism financing or evasion of sanctions. There is, for instance, evidence that terrorist groups have been experimenting with cryptocurrencies since 2014, including through social media campaigns aimed at raising Bitcoin for such groups.[38] Moreover, the absence of a finely-tuned regulatory framework for the ever-changing cryptocurrency markets makes it especially difficult to detect and deter bad actors.

A board and management also may ensure that their due diligence, account transaction monitoring, and suspicious activity reporting procedures are robust and efficacious with respect to dealings in cryptocurrency. It may be that the development of tailored transaction flags and employee trainings is appropriate given the special features of crypto-businesses. A board may also decide that it is not possible to mitigate fully the risks that cryptocurrency currently presents and decline to pursue the business.

Marijuana

The burgeoning marijuana industry in the United States also presents a set of unique challenges given the current rift between federal and state drug laws. Marijuana is a Schedule I controlled substance in the United States pursuant to the Controlled Substances Act ("CSA"), which prohibits, among other conduct, the production, sale, and distribution of marijuana.[39] However, with 10 states and the District of Columbia allowing recreational use of marijuana and a majority of states allowing use of marijuana for medical purposes, financial institutions are faced with addressing the challenges of legalisation at the state level even as it remains federally illegal. Pressures along the U.S. border also abound, as Canada recently legalised recreational consumption of marijuana and Mexico is considering similar legislation.[40]

The primary risk from the perspective of a financial institution is attachment of U.S. criminal liability under a theory of aiding and abetting a violation of or conspiring to violate the CSA and/or under AML statutes, which prohibit financial transactions involving the proceeds of "specified unlawful activity". "Specified unlawful activity" covers the manufacture, importation, sale, or distribution of a controlled substance, as defined under the CSA.[41]

For liability to attach to a financial firm under either U.S. drug laws or AML provisions, there must be: (1) a nexus between the marijuana-related business activities and the United States;[42] or (2) conduct that violates Canadian or other applicable local law.[43] The nexus requirement may be satisfied where a financial institution holds deposits for a marijuana-related business or trades in the securities of an entity engaged in U.S. marijuana-related activities.

As a statutory matter, the risk of federal prosecution in connection with marijuana-related activity in or touching the United States is plausible, but authorities have to date adhered to a policy of nonenforcement with respect to legitimate marijuana activities in states where the substance is legal. Meanwhile, marijuana-related activities in Canada bear a different risk profile: where an entity conducts marijuana-related activities only in Canada, and does so in full compliance with Canadian law, the provision of financial services to such a business should not violate U.S. federal criminal laws so long as there is no indication that the marijuana is being imported from or exported into the United States.

Financial institutions that are considering banking marijuana-related businesses, therefore, must consider not only their risk appetite in light of the potential for federal criminal liability with respect to U.S.-facing marijuana activities, but also reputational risks given that most major financial institutions have been leery of engaging with the industry. Key to any engagement with the marijuana industry is the implementation of an operational framework aimed at verifying compliance with applicable Canadian and U.S. laws, monitoring for marijuana-related activities that may touch the United States, and carrying out vigilant SAR compliance.

Managing Enterprise Risks

In managing risks associated with emerging industries, directors should ensure that their bank updates its policies and procedures in a way that accounts for the (1) particular AML risks associated with those sectors, (2) operational challenge of ensuring consistent treatment of these clients across business lines, and (3) potential for rapid changes in the legal and regulatory environment. While management is responsible for implementing an AML compliance framework tailored to the inherent challenges of higher-risk industries, directors can and should play an important role in understanding the risks, charting a strategic approach, and monitoring management's adherence to that strategy and the bank's risk appetite.

Directors should be sure to engage – and provide a credible challenge to – management in periodic discussions aimed at developing a shared understanding of how much risk the bank wishes to take, which will set the risk appetite across the organisation. Further, discussions about the opportunities presented in areas such as cryptocurrency and marijuana should include a robust debate regarding the attendant risks of those activities, both legal and reputational. These conversations should allow management to elevate risks to the board in a way that facilitates directors' ability to oversee the bank's risk-taking activities and hold management accountable for adhering to the risk governance framework. In providing active oversight, the board may question, challenge, and at times oppose decisions made by management that might cause the bank to exceed its risk appetite or even jeopardise safety and soundness.[44]

Conclusion

In sum, the responsibilities of bank directors extend well beyond assessing and monitoring SARs and discrete financial regulatory requirements. Developments since *Caremark* suggest that directors are being held to a higher standard, and should pay particular attention not only to repeated indicators of problematic activity, but also to risks in emerging sectors with the potential to disrupt the business and create regulatory headaches. Ongoing monitoring of AML risks should translate into effective enterprise risk management, including management of strategic and operational risks that implicate a bank's business model and reputation. Done properly, this approach should protect stakeholders while helping the bank anticipate and mitigate key risks.

Endnotes

1. Matthew L. Biben *et al.*, 2018/2019 Anti-Money Laundering Review and Outlook, Debevoise In Depth (Feb. 5, 2019), https://www.debevoise.com/~/media/files/insights/publications/2019/01/20190205_2018_anti_money_laundering_review_and_outlook.pdf. For purposes of this article, we use the term "AML" to refer to Bank Secrecy Act, AML, and sanctions rules for financial institutions, as well as related state laws and regulations.
2. Enforcement actions resulting in personal liability for compliance officers have become increasingly common. *See* Press Release, U.S. Dep't of Justice, Acting Manhattan U.S. Attorney Announces Settlement Of Bank Secrecy Act Suit

Against Former Chief Compliance Officer At Moneygram For Failure To Implement And Maintain An Effective Anti-Money Laundering Program And File Timely SARS (May 4, 2017), https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-settlement-bank-secrecy-act-suit-against-former; Press Release, U.S. Dep't of Justice, Rabobank NA Pleads Guilty, Agrees to Pay Over $360 Million (Feb. 7, 2018), https://www.justice.gov/opa/pr/rabobank-na-pleads-guilty-agrees-pay-over-360-million.

3. Emily Flitter *et al.*, *How Wells Fargo and Federal Reserve Struck Deal to Hold Bank's Board Accountable*, New York Times (Feb. 4, 2018), https://www.nytimes.com/2018/02/04/business/wells-fargo-fed-board-directors-penalties.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news/.
4. *See, e.g.*, Theodor Baums & Kenneth E. Scott, *Taking Shareholder Protection Seriously? Corporate Governance in the United States and Germany*, 53 Am. J. Comp. L. 31, 37 (2005) (explaining that the U.S. "fiduciary duty concept is derived from the common law of trusts, but has been modified in its application to the business context"); *CTS Corp. v. Dynamics Corp. of Am.*, 481 U.S. 69, 89 (1987) ("[n]o principle of corporation law and practice is more firmly established than a State's authority to regulate domestic corporations").
5. *In re Walt Disney Co. Derivative Litig.*, 907 A.2d 693, 745 (Del. Ch. 2005), *aff'd*, 906 A.2d 27 (Del. 2006) ("The fiduciary duties owed by directors … are the duties of due care and loyalty … and the duty of a director to act in good faith").
6. *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996) (duty to oversee and monitor); *Francis v. United Jersey Bank*, 432 A.2d 814, 822 (N.J. 1981) (duty to conduct regular review of financial statements); *Barnes v. Andrews*, 298 F. 614, 615 (S.D.N.Y. 1924) (duty to inquire into corporate affairs).
7. *Caremark*, 698 A.2d at 959.
8. *Id.* at 970.
9. *Id.* at 971.
10. *Id.*
11. *Louisiana Mun. Police Employees' Ret. Sys. v. Pyott*, 46 A.3d 313, 341 (Del. Ch. 2012) ("The decision to act and the conscious decision not to act are thus equally subject to review under traditional fiduciary duty principles").
12. *In re Wells Fargo & Co. S'holder Derivative Litig.*, 282 F. Supp. 3d 1074 (N.D. Cal. 2017).
13. *Id.* at 1082.
14. *Id.*
15. *Id.* at 1082–83.
16. *Id.* at 1083.
17. *Id.* at 1107-09 (citing *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, 370 (Del. 2006)).
18. *Id.* at 1088, 1107-09 (alteration in original).
19. On seemingly similar facts, a court considering shareholder derivative litigation against Citigroup held that plaintiffs failed to allege facts sufficient to meet the *Caremark* standard. *Oklahoma Firefighters Pension & Ret. Sys. v. Corbat*, No. 12151-VCG, 2017 WL 6452240 (Del. Ch. December 18, 2017).
20. *Caremark*, 698 A.2d at 970.
21. *See, e.g.*, KPMG LLP, *The three lines of defense* (2016), https://assets.kpmg/content/dam/kpmg/ca/pdf/2017/01/three-lines-of-defense-kpmg.pdf.
22. Off. of the Comptroller of the Currency, *Corporate and Risk Governance* (July 2016), at 42, 46–47, https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/corporate-risk-governance/pub-ch-corporate-risk.pdf.
23. *See* Matthew L. Biben, *So You Want to Join a Bank Board? Ask About AML Risk Oversight*, New York Law Journal (November 15, 2018), https://www.law.com/newyorklawjournal/2018/11/15/so-you-want-to-join-a-bank-board-ask-about-aml-risk-oversight/.
24. Fed. Fin. Insts. Examination Council, *BSA/AML Compliance Program – Overview*, Bank Secrecy Act Anti-Money Laundering Examination Manual, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_007.htm (last modified July 26, 2017).
25. *Id.*
26. Off. of the Comptroller of the Currency, *Director's Toolkit*, https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/directors-toolkit.html (accessed Feb. 18, 2019).
27. The Wolfsberg Group, *Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption* § 7, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf (last modified September 4, 2015).
28. *Id.*
29. Fin. Crimes Enf't Network, *Frequently Asked Questions: Conducting Independent Reviews of Money Services Business Anti-Money Laundering Programs* (September 22, 2006), https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-conducting-independent-reviews.
30. *See* Laura Akahoshi, Off. of the Comptroller of the Currency Notice # N18-002 (notice of charges for order of prohibition and assessment of a civil money penalty April 16, 2018), www.occ.gov/static/enforcement-actions/eaN18-002.pdf; Jesse Hamilton & Tom Schoenberg, *CEO of Bank That Hid Drug Cash Faces U.S. Criminal Probe*, Bloomberg (May 10, 2018).
31. Fed. Fin. Insts. Examination Council, *BSA/AML Compliance Program – Overview*, Bank Secrecy Act Anti-Money Laundering Examination Manual, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_007.htm (last modified July 26, 2017).
32. Fed. Trade Comm'n, *Western Union Admits Anti-Money Laundering Violations and Settles Consumer Fraud Charges, Forfeits $586 Million in Settlement with FTC and Justice Department* (January 19, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/western-union-admits-anti-money-laundering-violations-settles; Fin. Indus. Regulatory Auth., *Finra Fines LPL $2.75 Million for Complaint-Reporting and AML Program Failures* (October 30, 2018), https://www.finra.org/newsroom/2018/finra-fines-lpl-2-point-75-million-for-complaint-reporting-and-aml-program-failures.
33. *See* Aegis Capital Corp., Exchange Act Release No. 82956 (cease and desist order Mar. 28, 2018), https://www.sec.gov/litigation/admin/2018/34-82956.pdf; Sec. Exch. Comm'n, *SEC Charges Brokerage Firms and AML Officer with Anti-Money Laundering Violations* (May 16, 2018), https://www.sec.gov/news/press-release/2018-87.
34. Fed. Fin. Insts. Examination Council, *Office of Foreign Assets Control – Overview*, Bank Secrecy Act Anti-Money Laundering Examination Manual, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_037.htm (last modified July 26, 2017).
35. Michael del Castillo, *Jamie Dimon's Cryptocurrency Master Plan Swipes At Swift*, Forbes (Feb. 14, 2019),

https://www.forbes.com/sites/michaeldelcastillo/2019/02/14/jaime-dimon-finally-shows-jp-morgans-cryptocurrency-hand/#37f1a4b2e7ed. It is important to note, however, that JPM Coin has been described by many as being more akin to an in-house electronic payment system than a cryptocurrency. Unlike cryptocurrency, which is open, permission-less, and available to the public for download, JPM Coin will run on a private blockchain and operate within a closed, permissioned network. *See* Aaron Hankin, *JPM Coin is not a cryptocurrency, says crypto advocacy group*, MarketWatch (Feb. 15, 2019), https://www.marketwatch.com/story/jpm-coin-is-not-a-cryptocurrency-says-crypto-advocacy-group-2019-02-14.

36. *FinCEN, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

37. FATF, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, at 9–10 (June 2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

38. Zachary K. Goldman *et al.*, *Terrorist Use of Virtual Currencies*, Center for a New American Security (May 2017), lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.

39. *See* 21 U.S.C. § 801 *et seq.*

40. *See* Cannabis Act, S.C. 2018, c. 16 (2018) (Can.); Carrie Khan, *Mexico Looks To Be Next To Legalize Marijuana*, NPR (November 14, 2018), https://www.npr.org/2018/11/14/667699301/mexico-hopes-to-legalize-marijuana.

41. 18 U.S.C. § 1956(a)(1), (c)(7).

42. The nexus requirement emerges out of jurisprudence regarding the extraterritorial application of U.S. criminal statutes. *See*, *e.g.*, *United States v. Lawrence*, 727 F.3d 386, 395 (5th Cir. 2013) (a federal statute may apply extraterritorially under the "protective principle", which allows a nation to "enforce criminal laws wherever and by whomever the act is performed that threatens the country's security or directly interferes with its governmental operations").

43. U.S. AML provisions may apply where the proceeds at issue are obtained directly or indirectly from an "offense against a foreign nation", such as the manufacture, import, sale, or distribution of a controlled substance, as defined under the CSA. 18 U.S.C. §§ 1956(c)(7).

44. Off. of the Comptroller of the Currency, *Corporate and Risk Governance*, at 12 (July 2016), https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/corporate-risk-governance/pub-ch-corporate-risk.pdf.

Matthew Biben
Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
USA

Tel: +1 212 909 6606
Email: mbiben@debevoise.com
URL: www.debevoise.com

Matthew Biben is a member of the firm's White Collar & Regulatory Defense Group and co-leads the firm's Banking Industry Group. His practice focuses on problem solving; advising organisations and individuals and investigating, negotiating and litigating complicated regulatory and enforcement matters of all types with a particular focus on matters related to financial institutions and complex situations involving the government. He has extensive experience advising boards and senior management and his enforcement and advisory work has been wide-ranging. It includes internal investigations of both domestic and international matters relating to mortgages and other consumer products and securitisation claims and data privacy breaches, False Claims Act, Anti-Money Laundering and Bank Secrecy Act work. Prior to joining Debevoise, he served for 10 years in senior in-house roles at two of the largest financial institutions.

Meryl Holt Silverman
Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
USA

Tel: +1 212 909 6889
Email: mholt@debevoise.com
URL: www.debevoise.com

Meryl Holt Silverman is a litigation associate and a member of the White Collar & Regulatory Defense Group. Her practice focuses on internal investigations, regulatory inquiries and complex civil litigation. She has briefed and argued cases in the Second Circuit and the Southern District of New York, as well as in the New York State Appellate Division, First Department and the New York State Supreme Court. Before joining Debevoise, Ms. Holt Silverman served as the New York City Corporation Counsel Honors Fellow under Corporation Counsel Zachary W. Carter from 2016 to 2017. She clerked for the Hon. Joel M. Flaum of the U.S. Court of Appeals for the Seventh Circuit from 2015 to 2016.

Debevoise & Plimpton

Debevoise is a premier law firm with a market-leading anti-money laundering and trade sanctions compliance and enforcement practice. We provide expert and practical advice to a wide range of institutions – including securities broker-dealers, asset managers, and multinational banks – as well as leading industry associations. Our attorneys draw upon extensive experience (both from the private sector and in government). We closely follow the complex and fast-changing U.S., EU and Asian AML and sanctions regimes and work with clients in all types of adversarial proceedings, ranging from contentious regulatory examinations to administrative enforcement actions to civil and criminal litigation.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com