

ETHICS & COMPLIANCE

Now
Is the
Time
to Take
Action

CONSUMERS ARE SEETHING. Bankers—long regarded as paragons of integrity—have slipped from their pedestal. Congress continues to focus on tightening consumer protections. Formal enforcement actions addressing unfair and deceptive issues are becoming routine.¹ There could hardly be a better time to consider the connection between ethics and compliance.

This article begins with a discussion of the regulatory requirements and guidance regarding the establishment of a code of conduct or an ethics policy. The next section draws a distinction between compliance risk and complying with laws and regulations. The final segment offers suggestions for creating a code of conduct or ethics policy and provides a checklist for compliance officers whose scope of responsibility includes, or may include, oversight of compliance with such a code or policy.

Regulatory Requirements and Guidance

It is interesting to note that there are no regulatory requirements that a bank establish a code of conduct or an ethics policy. The Securities and Exchange Commission (SEC), pursuant to Section 406 of the Sarbanes-Oxley Act of 2002 (SOX), issued rules requiring certain companies, including banks, to disclose whether they have adopted codes of conduct or ethics policies, but those rules do not require the actual adoption of such a code or policy. The four bank regulatory agencies—the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, and the Office of Thrift Supervision (OTS)—have not issued regulations that specifically call for an ethics policy or a code of conduct. Of the four agencies, only the FDIC has issued guidance encouraging the development of such a code or policy.

SEC

The Securities and Exchange Commission (SEC) issued a regulation in January 2003² requiring each public company to disclose whether or not it has adopted a code of ethics that applies to certain of the company's key officers. The rules define "code

of ethics" as written standards that are reasonably designed to deter wrongdoing and to promote

- honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships
- full, fair, accurate, timely, and understandable disclosure in reports and documents that a company files with or submits to the SEC and in other public communications made by the company
- compliance with applicable laws, rules, and regulations
- the prompt internal reporting of any violations of the code of ethics to an appropriate person or persons identified in the code of ethics
- accountability for adherence to the code of ethics

Bank Regulatory Agencies

Although the bank regulatory agencies have not required banks to have codes of conduct or ethics policies, each agency has signaled its expectations that such codes or policies be adopted. With the exception of the FDIC, this expectation is not communicated directly to banks but rather indirectly through examination manuals, other publications, and speeches. For example, the *OCC Examination Handbook* directs examiners to ask the following:

- What written board-approved policies and procedures addressing internal control, risk assessments, and ethics/conduct are in place?
- Do audit or other control systems exist to periodically test for compliance with codes of conduct or ethics policies?
- Is compliance with established ethics/conduct policies periodically tested?

The OTS issued a regulatory bulletin on October 22, 2009,³ modifying the "Corporate Governance

“The board [of directors] has the responsibility for promoting a culture that encourages ethical conduct and compliance with applicable rules and standards.”

and Oversight by the Board of Directors” section of its *Examination Handbook*. The revised section now includes a portion identifying corporate governance best practices and specifically notes the adoption of a code of ethics as a best practice.

The Fed signaled its expectation in a 2008 supervisory letter⁴ addressing compliance risk management programs and oversight at large banking organizations. In this letter, the Fed noted, “The board [of directors] has the responsibility for promoting a culture that encourages ethical conduct and compliance with applicable rules and standards.”

In addition, in a commencement address in 2003, Roger W. Ferguson, Jr., vice chairman of the Federal Reserve Board, asked, “How can the organizations you will soon join manage legal risks and protect their reputations?” and provided this response:

It is here that I believe a well-crafted ethics policy and the means to monitor compliance can serve as a foundation. A solid program in support of ethical behavior, along with sound corporate governance, can act as an early warning system that raises concerns to senior managers and directors before they ripen into legal liability. A rigorous compliance program can also identify behavior that, while within the law, could tarnish the company’s reputation with very tangible consequences or equity value.

The most explicit guidance, however, was issued by the FDIC in the form of a Financial Institution Letter⁵ titled “Corporate Codes of Conduct—Guidance on Implementing an Effective Ethics Program.” This letter reminds banks supervised by the FDIC of the importance of an effective internal corporate code of conduct or written ethics policy. The letter states that

- A corporate code of conduct or ethics policy should be implemented to provide employees, officers, directors, and agents with specific guidelines on acceptable and unacceptable business practices.
- The policies should cover the entire organization, including subsidiaries and specific business activities unique to an institution.
- The corporate code of conduct or ethics policy should adopt provisions that explain the general prohibitions of the federal bank bribery law.
- Management should require bank employees, officers, directors, and agents to sign a written acknowledgement of the institution’s corporate code of conduct or ethics policy, including written acknowledgement of any subsequent material changes to the code or policy.

- Management should provide periodic training about its corporate code of conduct or ethics policy.
- Compliance with the policies should be monitored. Violators should be subject to specific and appropriate actions to deter wrongdoing, compel accountability, and promote adherence to the policy.

The letter also notes that the codes of conduct or ethics policies should address 12 issues, one of which is “observing applicable laws.” The letter includes the following list of laws and regulations that should be included in the codes and policies where applicable:

- Section 18(k) of the Federal Deposit Insurance Act (FDI Act)—authority to regulate or prohibit certain forms of benefits to institution-affiliated parties
- Part 359 of the FDIC rules and regulations—golden parachutes and indemnification payments
- Section 39(c) of the FDI Act—compensation standards
- Section 32 of the FDI Act—agency disapproval of directors and senior executive officers of insured depository institutions or depository institution holding companies
- Section 19 of the FDIC rules and regulations—reports and public disclosure of indebtedness of executive officers and principal shareholders to a state nonmember bank and its correspondent banks
- Sections 22(g) and (h) of the Federal Reserve Act—loans to executive officers of banks and extensions of credit to executive officers, directors, and principal shareholders of member banks
- The Federal Reserve Board’s Regulation O—loans to executive officers, directors, and principal shareholders of member banks
- Section 337.3 of the FDIC rules and regulations—limits on extensions of credit to executive officers, directors, and principal shareholders of insured nonmember banks
- Part 348 of the FDIC rules and regulations—management official interlocks
- Section 7(j) of the FDI Act and the Change in Bank Controls Act of 1978
- Section 737 of the Gramm-Leach-Bliley Act—bank officers and directors as officers and directors of public utilities
- Section 8(e) of the FDI Act—removal and prohibition authority
- Section 8(g) of the FDI Act—felony charge involving dishonesty or breach of trust as cause for suspension, removal, or prohibition

As the preceding discussion demonstrates, although the SEC and the banking agencies point to the need for ethical behavior in banks and expect some sort of policy

or program, the requirements and guidance vary widely. The distinctions are as follows: (1) applicability—the SEC requirement applies only to public companies and focuses on key officers; (2) formality—the FDIC is the only agency with formal guidance specifically addressing codes of conduct/ethics policies; and (3) content—what should be included in a code of conduct or an ethics policy is not articulated by all of the banking agencies and is not consistent when it is articulated. A review of the agency requirements and guidance also reveals that the focus is generally on employee-specific behaviors such as fraud, insider abuse, bribery, compensation, and loans to officers and directors, and the impact of the behavior on the banks. There is little guidance on codes of conduct or ethics as they relate to the treatment of consumers.

Consumer Protection and Compliance Risk

Consumer Protection

Regardless of their business model, size, or location, financial institutions must comply with myriad regulations designed to protect consumers. Complying with civil rights and consumer protection laws and regulations can be extremely challenging for several reasons: (1) there are many requirements; (2) some of the requirements are very detailed and prescriptive and include numerous interpretations by the agencies; (3) some requirements are vague, leaving room for a great deal of interpretation that has not been provided by the agencies; and (4) the requirements are constantly changing and expanding.

As shown in Table 1, the number of civil rights and consumer protection laws and regulations applicable to banks has grown consistently over the past four decades. Compliance officers are aware, some painfully so, that the recent crisis has spawned even more regulations designed to provide more protection for consumers. As Michael Collins, executive vice president of the Federal Reserve Bank of Philadelphia, noted in a 2004 article, “Throughout history, bubbles have been followed by significant contractions, which have in turn been followed by new laws, new rules, and new regulations designed to curb the excesses of the era just ended.”⁶

Compliance Risk

The Basel Committee on Banking Supervision defines compliance risk as “the risk of legal or regulatory sanctions, material financial loss, or loss of reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities”⁷ (emphasis added). With this definition in mind, compliance with laws, regulations, rules and other regulatory requirements is simply not enough to mitigate compliance risk. Compliance with ethical standards is also needed.

TABLE 1
Consumer Protection Timetable *

Fair Lending	1968
Flood Insurance	1968
Truth in Lending	1969
Fair Credit Reporting Act	1971
Consumer Leasing	1976
HMDA	1975
RESPA	1975
CRA	1977
EFTA	1978
FDCPA	1978
RTFP	1979
Credit Practices Rule	1986
Expedited Funds	1988
Branch Closings	1991
Telephone Consumer Protection Act	1991
Truth in Savings	1993
Interstate Branches	1994
Homeowners Protection Act	1999
Children's Online Privacy	2000
Privacy of Consumer Financial Information	2000
Disclosure of CRA Agreements	2000
SCRA	2003
CAN SPAM	2004
Limitations on Terms of Consumer Credit Extended to Servicemembers	2007
Protecting Tenants in Foreclosures	2009
Credit CARD Act	2009

*List is illustrative and not intended to be all-inclusive.

Compliance Officer Responsibilities

Given that compliance risk includes the risk of noncompliance with ethics standards and the regulatory expectation that banks have codes of conduct or ethics policies, compliance officers should examine their role in developing and ensuring compliance with codes of conduct, ethics policies, and core values.

In developing a code of conduct, a compliance officer might want to consider the SEC definition previously noted and the following definition from the International Federation of Accountants 2007 International Good Practice Guidance, “Defining and Developing an Effective Code of Conduct for Organizations”:

Principles, values, standards, or rules of behavior that guide the decisions, procedures and systems of an organization in a way that (a) contributes to the welfare of its key stakeholders, and (b) respects the rights of all constituents affected by its operations.

Many banks publish their codes of conduct or ethics policies on their Web sites; compliance officers might want



It is the right time for compliance officers to assist the bank in developing ethics standards and exercising oversight of compliance with the standards.

to review them to understand the variety of codes and policies. Many banks also articulate their core values—typically including service, teamwork, ethics, people, responsibility, integrity, customer focus, innovation, honesty, encouragement, accountability, and respect—on their Web sites.

If a decision is made that the responsibility for oversight of compliance with the bank's code of conduct, ethics policy, or values falls within the compliance officer's purview, the compliance officer should consider taking the following steps:

- Determine whether the SEC requirements apply to the bank.
- Determine the specific expectations of the bank's regulator.
- Add the responsibility for oversight of compliance with the code of conduct/ethics policy to the compliance officer's job description.
- Ensure that the bank's code of conduct/ethics policy identifies acceptable and unacceptable behavior.
- If the bank has articulated core values, ensure that the core values are consistent with and articulated within the code/policy.
- Assess the appropriateness of the coverage in the code of conduct/ethics policy—i.e., determine whether all employees are covered.
- Make certain the board of directors has approved the code of conduct/ethics policy.
- Include the risk of noncompliance with the code/policy in the assessments of compliance risk.
- Assist in the creation of business unit preventive and detective controls to prevent and identify noncompliance.
- Develop compliance department testing of compliance with the code/policy.
- If appropriate, coordinate with internal audit on the test-

ing for compliance with the code/policy.

- Establish reporting on the adequacy of controls to mitigate the risk of noncompliance with the code/policy.
- Ensure that an escalation process exists to raise issues regarding compliance with the code/policy.

When it comes to a code of conduct or an ethics policy, there is no time like the present for compliance officers to take a fresh look at the definition of compliance risk vis-à-vis their responsibilities. It is also the right time for compliance officers to assist the bank in developing ethics standards and exercising oversight of compliance with the standards. **BC**

ABOUT THE AUTHOR

Jeanine Catalano is a special adviser in Promontory's San Francisco office. Her work at Promontory focuses on all aspects of regulatory risk management, drawing on her more than three decades of financial institution regulatory risk management experience. Ms. Catalano earned an M.B.A. from Virginia Tech and a B.S. in finance from the University of Illinois. Ms. Catalano served in executive or senior compliance roles at two of the nation's largest lenders, where she was responsible for oversight of the enterprise-wide compliance testing function, the credit card compliance program, and developing compliance strategy and reporting for the home equity business unit. She also consulted for 12 years, focusing on assisting banks in responding to and preventing enforcement or other regulatory actions. Ms. Catalano held various positions with federal bank regulatory agencies, including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Office of Thrift Supervision. A portion of her agency work related to proposing and drafting enforcement actions as well as overseeing the management and resolution of severely troubled savings and loan associations. Reach her at jcatalano@promontory.com.

Endnotes

- ¹ There were 13 formal enforcement actions in the 18-month period ending June 30, 2009, that cited Unfair and Deceptive Acts and Practices violations.
- ² 17 C.F.R. 226.406.
- ³ RB 73-31.
- ⁴ SR 08-8 / CA 08-11.
- ⁵ FIL 105-2005.
- ⁶ Philadelphia Federal Reserve Bank, *SRC Insights*, First Quarter 2004.
- ⁷ Bank for International Settlements, *Compliance and the Compliance Function in Banks*.