Welcome to the Sunshine

May 31st, 2019 | and Nicole F. Munro

Life under a rock has its benefits – you probably don't get many houseguests, and you're never sunburned. But there are some drawbacks, too. The main one is that you definitely don't know what's been going on out here in the world of compliance. Well, it's spring here, and have we got some exciting not-so-new news for you!

In the summer of 2013, the Consumer Financial Protection Bureau advised in its Supervisory Highlights that it expects a company to have an effective Compliance Management System, adapted to its business strategy and operations. A CMS is how a company:

- establishes its compliance responsibilities;
- communicates those responsibilities to employees;
- ensures that responsibilities for meeting legal requirements and internal policies are incorporated into business processes;
- reviews operations to ensure that responsibilities are carried out and legal requirements are met;
- takes corrective action; and
- updates tools, systems, and materials, as necessary.

A CMS should be tailored to the size and complexity of an organization, must be risk-based and comprehensive (meaning that it should be integrated into operations and the entire life cycle of a transaction), and should be developed and refined over time. A company is expected to comply with federal consumer financial services laws from the very first day of operations. If you're new to this business, now that you're out from under your rock, you should expect the development of a comprehensive CMS to take 6-12 months or more. The truth is that you never stop developing and refining your CMS – just like you never stop developing and refining your business.

A CMS needs the following coordinated and interdependent control components:

- board and management oversight;
- a compliance program;
- a consumer complaint management program;
- a service provider management process; and
- an independent compliance audit function.

Here are some examples of what these components mean and what they should do:

Board and management oversight means that a company must:

- demonstrate clear expectations about compliance for the company and for third-party service providers;
- adopt clear policy statements about consumer compliance;
- appoint an appropriately qualified and experienced chief compliance officer and provide for other compliance officers with authority and accountability (In smaller or less complex entities where staffing is limited, a full-time compliance officer may not be necessary. However, management should have clear responsibility for compliance management, and compliance staff should be assigned to carry out this function.);
- establish a compliance function to set policies, procedures, and standards;
- allocate sufficient resources to the compliance function;
- address consumer compliance issues and associated risks of harm to consumers throughout product development, marketing, and account administration and through the handling of consumer complaints and inquiries;
- require audit coverage of compliance matters and review of the results of periodic compliance audits; and
- provide recurring reports of compliance risks, issues, and resolutions through a committee structure or to the board.

A **compliance program** consists of policies and procedures specifically addressing federal financial services law; training specifically addressed to compliance matters; and an ongoing process to monitor compliance, identify deficiencies, and take corrective action.

A **complaint management program** is to track, classify, and respond to consumer complaints and to identify and address the root causes of those complaints.

A **service provider management process** is for vendors and other service providers involved in activities subject to federal consumer financial laws and should include:

- due diligence to verify that a service provider understands and can comply with the law, including a review of the service provider's policies, procedures, internal controls, and training materials to ensure that the service provider conducts appropriate training and oversight of employees or agents that have consumer contact or compliance responsibilities;
- a contract with clear expectations about compliance and enforceable consequences for violations;
- internal controls and ongoing monitoring to determine whether the company is complying with the law; and
- requirements for prompt action to address identified problems fully.

A **compliance audit function** must be sufficiently independent and report to the board or to a committee of the board. The function should include an audit program that addresses compliance with all applicable federal consumer financial laws, schedules audit activities, requires audit reports to be distributed, and requires timely remediation of any deficiencies.

Any company attentive to its compliance obligations needs a CMS to address and prevent

violations of law and harm to consumers. But that's not all a company needs. In addition to a comprehensive CMS, some federal laws require written policies. If you've been under that rock since the '90s, you may have missed these requirements, too. Note that the requirements below are not all you have to know, and we have left out a lot of details, so meeting with your lawyer to see what you need might be a good idea.

In 1999, Congress enacted the Gramm-Leach-Bliley Act to provide for disclosures and substantive legal requirements related to the collection, use, and protection of personal information. Under the GLBA, the Federal Trade Commission established rules about safeguarding customer information (the "Safeguards Rule"). The rules require a company to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [the company's] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue."

In 2003, Congress enacted the Fair and Accurate Credit Transactions Act. One of the main purposes of FACTA was to provide consumers with protection against identity theft. Under FACTA, the FTC has enacted the Red Flags Rule and the Disposal Rule.

The Red Flags Rule requires a creditor that offers or maintains covered accounts to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. A "red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Under the FTC's Disposal Rule, any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of that information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. Examples of proper disposal measures include "implementing and monitoring compliance with policies and procedures that require" certain methods of destroying information. In addition, "for persons subject to the [GLBA] and the [Safeguards Rule], incorporating the proper disposal of consumer information as required by [the Disposal Rule] into the information security program required by the Safeguards Rule" is also acceptable.

In 2010, the final Furnisher Rule and Guidelines were published by several government agencies. The FTC's rule and guidelines apply to any entity that furnishes consumer report information. The first part of the rule requires that furnishers: (1) have reasonable policies and procedures to ensure the accuracy and integrity of information furnished to consumer reporting agencies; and (2) conduct a reasonable investigation of direct disputes from consumers. The rule sets out the basic requirements, and the guidelines set out flexible standards for the furnisher to consider and implement.

Maybe you're still thinking of heading back home, under your trusty rock. Don't bother. Hiding your head in the sand or under a rock is not going to satisfy the CFPB or the FTC when they come knocking. Truth be told, developing and refining your CMS is not only good for compliance, but it's also good for business. Welcome to the sunshine!