sound training program is a bank’s first line of defense to assure that its compliance program will meet regulatory scrutiny and avoid civil liability. Furthermore, certain regulations require employee training. However, the training should also match up with the bank’s size and complexity and the types of products and services that it offers. Let’s first look at some critical training areas and then consider possible training solutions.

BSA/AML. According to the BSA/AML regulations, part of an effective compliance program is training for “appropriate” personnel. According to the exam manual, training should include regulatory requirements and the bank’s internal BSA/AML policies, procedures and processes. It should be tailored to the person’s specific responsibilities. In any event, an overview should be given to new staff during employee orientation.

Virtually every department is touched in some way by BSA/AML. For example, tellers must be aware of Currency Transactions Report requirements and recordkeeping for money orders and wires. New accounts staff, trust department and loan officers must have a thorough understanding of the bank’s customer identification program requirements. All departments must be prepared to identify suspicious transactions for SARs.

The board and senior management should be informed of changes and new developments in the BSA. Although the board may not require the same in-depth training that is provided to employees, since it is responsible ultimately for the bank’s compliance program, the board must have a good understanding of the requirements, the ramifications of noncompliance and the risks posed to the bank.

Training should be ongoing and incorporate current developments and changes to BSA as well as bank changes to policy and procedures. It should be tailored to the risk profile of the bank. Banks should document their training programs including the dates of training sessions along with attendance records. Employees should be tested on their comprehension at the end of the training.

Fair Lending. Although the Equal Credit Opportunity Act and other fair lending statutes and regulations do not explicitly mandate employee training, virtually all enforcement actions and consent orders include a training component. Remember that these are not consumer regulations but rather “civil rights” ones. The prohibitions against improper discrimination apply to commercial as well as to consumer and residential mortgage loans. Furthermore, a teller or new accounts officer may inadvertently take an “application” as defined in Regulation B or, worse yet, discourage an application. For example, a person may inquire about the bank’s auto loan rates. If the bank employee asks for the make and sales price of the car in order to quote the rate, then that is still an inquiry. But if the employee finds out that the consumer has filed a bankruptcy proceeding and tells her not to bother applying, then there has been an adverse action. Thus, any employee who responds to an inquiry about loan products needs to understand the fine line between providing helpful info to a prospective customer and taking an application.

It is particularly important that the board of directors also receive fair lending training. The board sets policy for the bank and should also assure that the bank’s culture is consistent with fair lending. Remember that creditors are rarely found guilty of overt discrimination. Rather, the pricing policies (or more likely the non-existence of such policies) may lead an examiner to find that the institution’s actions have a “disparate impact” on protected classes. If the board does not have a sound understanding of fair lending, it can’t make good decisions relating to rate sheets and pricing for loans.

Privacy/security. Under the Gramm Leach Bliley Act, banks must have strong security procedures to protect consumers from unauthorized release (or breach) of their personal protected information. The Security Guidelines require a financial institution to train staff to prepare and implement its information security program. The institution should consider providing specialized training to ensure that personnel sufficiently protect customer information in accordance with its information security program. An institution should:

- Train staff to recognize and respond to schemes to commit fraud or identity theft, such as guarding against pretext calling;
- Provide staff members responsible for building or maintaining...
computer systems and local and wide-area networks with adequate training, including instruction about computer security; and

- Train staff to properly dispose of customer information.

Here is a link to an interactive training program from the FTC on information security. While this was created for businesses generally, it is a readily accessible, easy to understand program on the basics of customer information security: [http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html](http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html)

**Fair Credit Reporting Act.** Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (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. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. The Program should identify and have procedures to detect, and then respond appropriately to red flags that suggest identity theft could be occurring. The Identity Theft Red Flags rule also clearly requires creditors to train staff as necessary. Thus, employees must understand the policy and carry out the Program.

**Sexual Harassment.** The Equal Employment Opportunity Act prohibits discrimination in any aspect of employment. It applies to employers with 15 or more employees. One area of potential discrimination is sexual harassment. This includes practices ranging from direct requests for sexual favors to workplace conditions that create a hostile environment for persons of either gender, including same sex harassment. (The “hostile environment” standard also applies to harassment on the bases of race, color, national origin, religion, age, and disability.)

One of the best ways to protect against a claim of “hostile environment” is to assure that all employees are appropriately trained to avoid behaviors that could create liability for the employer.

**Other areas.** The specific laws discussed above are only the tip of the iceberg with regard to topics worthy of training. Staff must be trained to understand and implement all bank policies that apply to or affect their product line. Furthermore, all employees should be familiar with the bank’s “code of conduct” dealing with conflicts of interest, Bank Bribery Act, and insider transactions (Regulations O and W).

**Implementation.** There are many sources for bank training, including, of course, the programs offered through the IBAT Education Foundation! In addition, there are PowerPoint programs on regulator web sites. For example, the FFIEC produced a PowerPoint in 2003 to introduce the changes to HMDA: [http://www.ffiec.gov/hmda/powerpoint.htm](http://www.ffiec.gov/hmda/powerpoint.htm). The FDIC has videos on its web site to train bank employees on deposit insurance: [http://www.fdic.gov/deposit/deposits/video/videos.html](http://www.fdic.gov/deposit/deposits/video/videos.html)

Whatever resource is used for the subject matter of the (Continued on page 35)
training, be sure that attendees sign a registration list. Retain this and be prepared to show examiners this proof of which employees have received training. Be sure that training on critical laws includes testing. Select training materials that are appropriate for your bank and its mix of products and size. Finally, have a little fun! Include small prizes for attendees along with refreshments (of a non-alcoholic nature!). Remember that good training can protect the bank from bad examinations and potential lawsuits.

Analytics the Community Way
In instances where risk managers may prefer it or regulators may require it, a full-blown deposit analysis might be performed in an attempt to glean greater predictability in the rate sensitivity and decay characteristics of certain accounts. For a “typical” community bank, however, such an analysis can often prove to be cost prohibitive and it’s not a certainty that such a statistical exercise would result in a banker knowing his customers any better than he already does. To the extent that they are able, we encourage all risk managers to perform their own historical internal analysis of deposit rate and balance behavior through past business cycles and rate environments. At the very least, it can add another window of insight into the banker/customer relationship. It is, in fact, this relationship that bankers have with their communities for which there is no statistical substitute. As a community banker, no one knows your customers better than you.

interest rates cont’d from page 14
Trade area and competitive environment can account for significant differences in depositor preferences. Thus, simply defaulting to a predetermined treatment for NMD’s may or may not accurately reflect the true impact that changing interest rates may have on the holders of non-maturing deposits.