# acxell

ADVISOR

Spring 2021


5 TIPS FOR FAIR LENDING COMPLIANCE

SHOULD YOUR BANK USE THIRD-PARTY VENDORS?

ONLINE ACCOUNT OPENING: MANAGING THE RISK

BANK WIRE

acxell

**www.acxellrms.com 877.651.1700**

# 5 TIPS FOR FAIR LENDING COMPLIANCE

Community banks need to develop and follow fair lending practices; providing customers with nondiscriminatory access to credit is, of course, the right thing to do. What's more, violations of fair lending laws and regulations can result in costly litigation and enforcement actions, hefty monetary penalties and serious reputational damage.

## WHAT ARE THE LAWS?

The two primary fair lending laws are the Fair Housing Act (FHA) and the Equal Credit Opportunity Act (ECOA). The FHA prohibits discrimination in residential real estate-related transactions based on race or color, national origin, religion, sex, familial status (for example, households with one or more children under 18, pregnant women, or people in the process of adopting or otherwise gaining custody of a child), or handicap.

Similarly, the ECOA prohibits discrimination in credit transactions based on race or color, national origin, religion, sex, marital status, age (assuming the applicant has the capacity to contract), an applicant's receipt of income from a public assistance program, or an applicant's good faith exercise of his or her rights under the Consumer Credit Protection Act.

The Home Mortgage Disclosure Act (HMDA) requires certain lenders to report information about mortgage loan activity, including the race, ethnicity and sex of applicants. Finally, the Community Reinvestment Act (CRA) provides incentives for banks to help meet their communities' credit needs.

## HOW CAN YOU COMPLY?

Here are five tips for developing an effective compliance program:

**1. Conduct a risk assessment.** Conduct a thorough assessment to identify your bank's fair lending risks based on its size, location, customer demographics, product and service mix, and other factors. This assessment can pinpoint the bank's most significant risks. It also can reveal weaknesses in the bank's credit policies and procedures and other aspects of its credit operations. It's particularly important to examine the bank's management of risks associated with third parties, such as appraisers, aggregators, brokers and loan originators.


**2. Develop a written policy.** A comprehensive written fair lending policy is key to help minimize your bank's risks. And by demonstrating your commitment to fair lending, this document can go a long way toward mitigating the bank's liability in the event of a violation. The policy should cover all of the bank's products, services and credit operations and provide details about which practices are permissible and which aren't.

**3. Analyze your data.** Analyzing data about your lending and other credit decisions is important for two reasons: First, it's the only way to determine whether disparities in access to credit exist for members of the various protected classes. These disparities don't necessarily signal that unlawful discrimination is taking place — but gathering this data is the only way to make this determination.

> IT'S PARTICULARLY IMPORTANT TO EXAMINE THE BANK'S MANAGEMENT OF RISKS ASSOCIATED WITH THIRD PARTIES, SUCH AS APPRAISERS, AGGREGATORS, BROKERS AND LOAN ORIGINATORS.

Second, lending discrimination isn't limited to disparate treatment of protected classes. Banks are potentially liable under the FHA and ECOA if their lending practices have a disparate *impact* on protected classes. For example, a policy of not making single-family mortgage loans under a specified dollar amount may disproportionately exclude certain low-income groups, even though the policy applies equally to all loan applicants. Banks can defend themselves against allegations of discrimination based on disparate impact by showing that the policy was justified by business necessity and that there was no alternative practice for achieving the same business objective without a disparate impact.

**4. Provide compliance training.** Even the most thorough, well-designed policy won't be worth the paper it's printed on unless you provide fair lending compliance training for bank directors, management and all other relevant employees (and evaluate its effectiveness). Indeed, lack of training is a red flag for bank examiners. (See "Discrimination risk factors" above.)

**5. Monitor compliance.** You'll need to monitor your bank's compliance with fair lending laws and promptly address any violations or red flags you discover. You can do this by, among other things, performing regular data analysis, monitoring and managing consumer complaints, keeping an eye on third-party vendors, and conducting periodic independent audits of your compliance program (by your internal audit team or an outside consultant).

## DISCRIMINATION RISK FACTORS

A useful source of guidance on fair lending compliance is the Interagency Fair Lending Examination Procedures used by federal financial agencies. Among other things, the guidelines list the following compliance program discrimination risk factors:

- Overall compliance record is weak,
- Legally required monitoring information is nonexistent or incomplete,
- Data or recordkeeping problems compromise the reliability of previous examination reviews,
- Fair lending problems were previously found in one or more products or subsidiaries, and
- The bank hasn't updated compliance policies and procedures to reflect changes in law or in agency guidance.

If any of these problems are present in your institution, it's important to rectify them as soon as possible. That way, you'll avoid penalties and at the same time contribute to fair lending practices.

## REDUCE YOUR RISK

Fair lending laws are complex, and guidance can sometimes be ambiguous. Although a full discussion of the subject is beyond the scope of this article, the five tips outlined here are a good start in helping you evaluate the effectiveness of your fair lending compliance program. ■

# SHOULD YOUR BANK USE THIRD-PARTY VENDORS?

In the uncertain economy resulting from the COVID-19 pandemic, community banks continue to streamline operations, improve efficiency and eliminate waste so that they can survive — and thrive. To help in this process, they're increasingly turning to outside vendors to provide specialized services beyond the bank's usual offerings. If your bank uses third-party vendors, though, you need to be aware of the ins and outs.

## EVALUATE LIABILITY

Outsourcing to a third party doesn't relieve a bank from responsibility and legal liability for compliance or consumer protection issues. And as banks and vendors increasingly rely on evolving technologies to deliver products and services, their exposure to ever-changing cybersecurity risks demands constant vigilance.

Even if you have a solid vendor risk management program in place, you'll need to review it periodically. Banking regulators expect your program to be "risk-based" — that is, the level of oversight and controls should be commensurate with the level of risk an outsourcing activity entails. But here's an important caveat: That risk can change over time. Some vendors, such as appraisal and loan collection companies, have traditionally been viewed as relatively low risk. But in today's increasingly cloud-based world, any vendor with access to your IT network or sensitive nonpublic customer data poses a substantial risk.

## ASSESS RISK

Here are some ways to review your vendor risk management program:

**Conduct a risk assessment.** Determine whether outsourcing a particular activity is consistent with your strategic plan. Evaluate the benefits and risks of outsourcing that activity as well as the service provider risk. This assessment should be updated periodically.

Generally, examiners expect a bank's vendor management policies to be appropriate in light of the institution's size and complexity. They also expect more rigorous oversight of *critical* activities, such as payments, clearing, settlements, custody, IT or other activities that could have a significant impact on customers — or could cause significant harm to the bank if the vendor fails to perform.

**Thoroughly vet your service providers.** Review each provider's business background, reputation and strategy, financial performance operations, and internal controls. The depth and formality of due diligence depends on the risks associated with the outsourcing relationship and your familiarity with the vendor. If your agreement allows the provider to outsource some or all of its services to subcontractors, be sure that the provider has properly vetted each subcontractor. The same contractual provisions must apply to subcontractors and the provider should be contractually accountable for the subcontractor's services.

**Diversify vendors.** Using a single vendor may provide cost savings and simplify the oversight process, but diversification of vendors can significantly reduce your outsourcing risks, particularly if a vendor has an especially long disaster recovery timeframe.

**Ensure contracts clearly define the parties' rights and responsibilities.** In addition to costs, deliverables, service levels, termination, dispute resolution and other terms of the outsourcing relationship, key provisions include compliance with applicable laws, regulations and regulatory guidance; information security; cybersecurity; ability to subcontract services; right to audit; establishment and monitoring of performance standards; confidentiality (in the case of access to sensitive information); ownership of intellectual property; insurance, indemnification and business continuity; and disaster recovery.

**Review vendors' disaster recovery and business continuity plans.** Be sure that these plans align with your own and are reviewed at least annually, and that vendors have the ability to implement their plans if necessary.

**Monitor vendor performance.** Monitor vendors to ensure they're delivering the expected quality and quantity of services and to assess their financial strength and security controls. It's particularly important to closely monitor and control external network connections, given the potential cybersecurity risks.

**Conduct independent reviews.** Banking regulators recommend periodic independent reviews of your risk management processes to help you assess whether they align with the bank's strategy and effectively manage risks posed by third-party relationships. The frequency of these reviews depends on the vendor's risk-level assessment, and they may be conducted by the bank's internal auditor or an independent third party. The results should be reported to the board of directors.

### STAY AWARE

Having a robust vendor risk management program in place at your bank is the key to benefiting from vendors' specialized skills and abilities while avoiding legal and regulatory problems. We can help you stay on top of the latest regulations and rules pertaining to third-party vendor use. ■

# ONLINE ACCOUNT OPENING: MANAGING THE RISK

In recent years, banking customers have increasingly relied on electronic banking tools to open accounts, make deposits, transfer funds and otherwise manage their money — and the COVID-19 pandemic has accelerated this trend. All of these activities increase an institution's Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance risks, particularly the opening of online accounts. So, while offering these conveniences can be attractive to current and prospective customers, you'll need to implement policies, procedures and controls to mitigate the risk.

### RECOGNIZING RISK FACTORS

In its BSA/AML Manual, the Federal Financial Institutions Examination Council (FFIEC) emphasizes that accounts opened online — that is, without face-to-face contact — pose a greater risk for money laundering and terrorist financing because:

- It's more difficult to positively verify the applicant's identity,
- The customer may be outside the bank's targeted geographic area or country,

- Customers — particularly those with ill intent — may view online transactions as less transparent,
- Transactions are instantaneous, and
- Online accounts may be used by a "front" company or unknown third party.

In light of this enhanced risk, the FFIEC cautions banks to consider how an account was opened as a factor in determining the appropriate level of account monitoring.

## MINIMIZING RISKS

To reduce the risks associated with online account opening, banks should develop an effective customer identification program (CIP) and ongoing customer due diligence (CDD) processes as part of a robust, risk-based BSA/AML compliance strategy.

To comply with CIP requirements, an individual opening an account must provide, at a minimum, his or her name, date of birth, address and taxpayer identification number (or other acceptable identification number for non-U.S. persons). In addition, if an account is opened for a legal entity — such as a corporation, partnership or LLC — the bank must verify the identities of the entity's beneficial owners.

## VERIFYING APPLICANTS' IDENTITIES

A significant challenge in electronic banking is verifying the identity of someone opening an account online (including a person opening an account on behalf of a legal entity). For in-person transactions, bank personnel often examine identification documents, such as driver's licenses or passports, but this may not be possible for accounts opened online.

For online transactions, banks should develop reliable nondocumentary methods of verifying an individual's identity. These may include comparing the information provided at account opening with information from a credit reporting agency, public database or other source. They also may include contacting the person (for example, calling them at work or sending them a piece of mail they must respond to), checking references with other financial institutions, obtaining a financial statement, or asking "out of wallet" questions, such as previous addresses, former employers or mortgage loan amounts.

The bank should develop alternate or backup verification methods for situations in which one of these methods fails. For example, if there's an identification mismatch, the applicant may be required to bring identification in person to a bank branch.

In addition, as with accounts opened in person, the bank should check the person's name against lists of known or suspected terrorists or terrorist organizations maintained by the Office of Foreign Assets Control. It's also a good idea, for ongoing monitoring and CDD purposes, to collect information about the purpose of the account, the occupations of the account owners and the source of funds.

## DUE DILIGENCE

After an account is opened online and the applicant's identity is verified, you'll want to conduct ongoing customer due diligence. That means, among other things, monitoring account activity for unusual or suspicious activities. ■

# BANK WIRE

## CAA PROVIDES COVID-19 RELIEF FOR BANKS

The Consolidated Appropriations Act (CAA), passed in late December 2020, contains a variety of COVID-19 relief provisions, including a second round of stimulus payments to individuals, enhanced unemployment benefits, and expansion of the Paycheck Protection Program (PPP). The act also offers some bank-specific relief. For example, it:

- Delays the compliance deadline for the current expected credit loss (CECL) accounting standard until the earlier of 1) the first day of the bank's fiscal year that begins after termination of the COVID-19 public health emergency, or 2) January 1, 2022; and
- Extends the time during which banks may elect to temporarily suspend troubled debt restructuring (TDR) accounting for certain COVID-19-related loan modifications until the earlier of 1) 60 days after the public health emergency ends, or 2) January 1, 2022.

It also establishes a $9 billion fund to provide low-cost, long-term capital investments to qualifying banks. To qualify, they need to be community development financial institutions or minority depository institutions. ■

## SBA GUIDANCE ON PPP LOANS

After the CAA authorized "second-draw" forgivable PPP loans, the Small Business Administration (SBA) and Treasury Department issued rules for these loans. Among other things, the rules clarify that: the SBA will guarantee 100% of second-draw loans; no collateral or personal guarantees will be required; the interest rate will be 1%, calculated on a noncompounding, nonadjustable basis; maturity will be five years; and all loans will be processed by lenders under delegated authority.


It may rely on borrower certifications to determine the borrower's eligibility and use of loan proceeds. (Note: The borrower must substantiate compliance with eligibility requirements by the time they submit a forgiveness application.) ■

## SIMPLIFIED PPP FORGIVENESS APPLICATION

The CAA simplifies the forgiveness application for businesses that borrow less than $150,000. These borrowers will submit a one-page application that includes the total loan value, the estimated portion of the loan spent on payroll, and the number of employees retained as a result. ■

## FINTECH PARTNERSHIP GUIDE

Community banks are increasingly partnering with "fintech" companies to offer their customers access to the latest banking technology tools. But these partnerships are fraught with practical and regulatory compliance challenges. Recently, a member of the Federal Reserve Board announced that the Fed would work with other banking agencies to develop a fintech vendor due diligence guide for community banks as well as enhanced interagency guidance for third-party risk management. This guidance is expected to "eliminate the need for community banks to navigate multiple supervisory guidance documents on the same issue" and "enhance clarity on supervisory expectations for community bank partnerships with fintech companies." ■

**acxell** ("acxell") has been meeting the specific risk management needs of community banks of all sizes since 1991. As a high quality and affordable alternative to other firms, acxell provides internal audit, regulatory compliance, BSA/AML, information technology, SOX/FDICIA and enterprise risk management review services and software. acxell is exclusively dedicated to the banking industry, providing clients with dedicated, focused and hand-held services reflective of a wide range of skills, experience and industry expertise. As a Firm, we have also been proactive in assisting our clients with the designing, implementation and testing of the internal control environment to assist management with the attestation requirement under the Sarbanes-Oxley Act.

acxell's uniqueness is characterized by its experienced staff and partners. Their hands-on involvement on each engagement provides our clients with a wide range of skills, experience and industry expertise. We employ the use of Subject Matter Experts — designated individuals performing audits in their specific field of expertise. The use of such professionals provides a unique value-added approach that is both efficient and productive.

We believe that a significant aspect of our services is our degree of involvement and responsibility to assist management by making suggestions for improvement, keeping them informed of professional developments and by acting as an independent counsel and sounding board on general business matters and new ideas.

We pride ourselves in our ability to provide effective and practical solutions that are commensurate with our clients' needs by emphasizing high-quality personalized service and attention. Our services are truly customized.

*For* **Solutions** *to your risk management needs, please contact our service coordinators at (877) 651-1700, or log-on to www.acxellrms.com to learn more.*

www.acxellrms.com

Headquarters:
646 US Highway 18
East Brunswick, NJ 08816

Offices:
New York, NY
Philadelphia, PA
Chicago, IL
Miami, FL