ProBank Austin

ProBank Statement of Qualifications

To Provide Consumer Compliance Consulting Expertise to the Online Lending Industry

As of March 2017

ProBank Austin
The 1000 Building
6200 Dutchmans Lane, Suite 305
Louisville, KY 40205

Contact
Martin (Marty) T. Mitchell, CRCM
mmitchell@probank.com
502.479.5258 (Direct)

An Employee-Owned Small Business Serving the Financial Industry for 39 years

ProBank Austin

6200 Dutchmans Lane, Suite 305
Louisville, KY 40205
(502) 451-6633

216 Centerview Drive, Suite 225
Brentwood, TN 37027
(615) 370-5006

7205 West Central Avenue
Toledo, OH 43617
(419) 841-8521

www.probank.com
(800) 523-4778

March 2017

Dear Online Lender:

I appreciate your interest in our company and we are pleased to provide this information packet. We have developed a proven approach to assist online lenders prepare to operate confidently within the current consumer compliance regulatory environment.

Please allow me to provide a brief introduction to our company; we too are a true small business and know what it means to be good stewards of your budget. Founded in 1978, ProBank has been employee owned since 2003. Throughout our 39-year history, we have remained the leader in providing consulting and education services to the financial industry. We began educating, consulting, auditing, and advising online lenders in 2013 and have since developed relationships with a wide variety of lenders and their partnering financial institutions.

Addressing Your Team's Needs

Upon engagement, we will:

- Work with your team to develop the compliance management program policies necessary to partner with a federally regulated institution while recognizing your unique business niche
- Provide audit and review services to promote and validate effective compliance controls and monitoring for your lending platform
- Meet or exceed your expectations as well as those of your partnering bank with regards to documenting an appropriate Compliance Management Program (CMP), corrective action taken on identified issues, and validation such action is sustained over time
- Establish a cooperative, mutually beneficial relationship

The Specifics

Consider this an Executive Summary of our approach. This document outlines in detail the phases and provides an overview of our services designed specifically for online lenders.

- Compliance Management Program (CMP) Policies Review – Completed prior to going live

- Information Technology and Information Security Policies and Program, Business Continuity Plan, Audit, Vulnerability Testing, and Social Engineering – Work begins prior to going live and continues throughout relationship

- Lending Review (Transactional Testing) for Compliance with Applicable Lending Rules and Regulations – Normally conducted within 60 days of going live; may be accelerated or delayed based on volume

- Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Independent Review – Normally conducted concurrent with transactional testing

- Annual Review – This review combines all the necessary components listed above at the one-year point

- Fair Lending/Non-Discrimination Analysis

Why Choose ProBank

Providing consulting and education services to the financial industry is what we do. We conduct 30 to 50 consumer compliance reviews each and every month for institutions and businesses across the country. We are unique in being a small business with true professionals, having decades of experience in all facets of the consumer compliance rules and regulations governing your business. Our internal education staff produces training materials long touted as the industry best while also conducting nearly 1,000 seminars each year on these very topics.

Our approach is a personal one. We have a singular, dedicated relationship manager (Robert “Bob” Mullenbach) for all of our online lending work. This enables us to best understand your needs and also the requirements of the partnering bank. Bob will work directly with your team and will manage our internal resources to assure the right fit of our staff to your needs. He will also manage the timeline and keep the partnering bank up to date. With ProBank, you will work directly with experienced professionals who employ all necessary resources to meet your service expectations.

We appreciate the opportunity to provide our credentials. As an employee-owned business, we are understandably proud of what we do and hold ourselves to the highest of standards. Although we operate nationally, we are a small business focused on one client at a time. I welcome any opportunity to answer your questions or further discuss how we may assist you.

Very truly yours,

Martin T. Mitchell, CRCM
Managing Director
mmitchell@probank.com
502.479.5258

Table of Contents

Section I

ProBank Austin

Our Firm at a Glance

Since 1978 ProBank Austin (ProBank) has been the leader in providing consulting and educational services to the financial industry. Our staff includes former bank regulators (compliance as well as safety and soundness examiners), bankers, attorneys, financial analysts, and accountants. Our senior consultants have decades of experience within their fields and are adept at not only conducting formal reviews and audits but also providing the right mix of education, advice, and consulting to meet our clients' needs.

Our clients are diverse and nationwide. They include banks, credit unions, law firms, federal and state regulatory agencies, and major insurance companies.

Our services are also wide ranging to include:

- Merger and Acquisition
- De Novo Charter
- Branching
- Loan Review Services
- Internal and IT Audits
- Trust Audits
- Capital Plans
- Asset-Liability Management and Liquidity Reviews
- Consumer Compliance Rules and Regulation Reviews
- CRA and Fair Lending Reviews
- Sarbanes-Oxley Section 404 Assistance
- Litigation Consulting
- Expert Witness Service
- Investment Banking Services
- Stock Appraisals
- Fairness Opinions
- New Bank Charters
- Branch and Premises Feasibility Studies
- Policy Development
- Quality Control and Quality Assurance Audits
- Strategic Planning
- Due Diligence Reviews
- Director and Officer Training
- Independent BSA/AML Reviews
- Educational Training through Compliance Schools, Conferences, Seminars, Webinars, and In-House Training

Through our services, we are able to educate, consult, audit, and advise clients. We are proud of being an employee-owned company and take a personal approach when assessing the needs of each individual client.

Section II
ProBank Approach

Phase I: Compliance Policies

Engagement, Objective, and Approach for Compliance Policies

At the onset of our relationship with your company, we will conduct an assessment of your existing compliance policies to evaluate whether they are comprehensive and conform to the requirements of applicable regulations and/or expectations of industry guidance.

As provided by management, the policies to be reviewed are as follows:

- Consumer Financial Privacy Policy
- Electronic Funds Transfer Act Policy
- Identity Theft Protection Policy
- Financial Information Exception for Obtaining and Using Medical Information Policy
- Bank Secrecy Act/Anti-Money Laundering Policy
- Equal Credit Opportunity Act ~ Regulation B Policy
- Truth-in-Lending Policy ~ Regulation Z
- Fair Credit Reporting Act Policy
- Electronic Signatures in Global and National Commerce Act Policy
- Fair Lending Plan
- Unfair, Deceptive, or Abusive Acts or Practices Policy
- Consumer Debt Collection Policy
- Loan Underwriting Policy*
- Complaint Policy
- Servicemembers Civil Relief Act Policy
- Vendor Management Policy
- Privacy Policy
- Marketing Policy
- Military Lending Act

**The "Loan Underwriting Policy" will be reviewed for compliance factors only and will not encompass asset quality underwriting criteria.*

In addition, ProBank will review the following loan document set (for compliance purposes only) including but not limited to:

- Credit Application (virtual review of customer/consumer experience required or deemed incomplete)
- Notice of Action Taken
- Promissory Note
- Truth-in-Lending Disclosure
- All other consumer-facing disclosures (hard and soft)

The engagement product will include a written assessment of each policy outlining any recommendations for additional policy considerations and disclosure review results. This phase of the engagement is typically conducted off-site.

Phase 2 – Information Security/ Information Technology Policies

Part A – Services for Information Security Program/Technology Policies and Business Continuity Plan

Information Security Program/Technology Policies

ProBank will review any documentation associated with Information Security, Information Technology, risk assessments, vendor oversight and business continuity planning the Company currently maintains. After review of the documentation, ProBank will either update the Company's Information Security Program to include missing components or if the documentation provided by the Company is limited, ProBank will take the Company's information and insert the information into a new document prepared by ProBank. The scope of the Information Security Program, which will also address Information Technology controls used by the Company, will include the following components:

- Information Security Policy
- Information Classification
- Privacy Policy
- Physical Security
- Disposal of Customer Information
- Cybersecurity Controls
- Loan Origination System
- Access/Authentication Security Controls
- Remote Access Policy
- Virtual Private Network Policy
- Mobile Device Policy
- Vendor Management Policy
- Record Retention Requirements
- Cybersecurity Insurance Coverage
- Annual Testing
- Acceptable Use Policy – Electronic Media
- Internet Use Policy
- Social Networking Policy
- Information Security Training Policy
- Reporting to the Board of Directors
- Incident Response Procedures

The following Cloud Adoption/Security components will be addressed in the Policy in the Risk Assessment portion of the documents:

- Cloud-computing service model(s) used by the Company
- Cloud-computing deployment model used by the Company
- Business Impact and Risk
- Governing the Cloud
- Contractual Compliance between the Service provider and Customer

- Control Issues Specific to Cloud Computing

The Information Systems/Security Risk Management Program portion of the engagement will address review and/or development of the following documentation:

- Physical Security Threats/Controls Risk Assessment
- Service Provider Due Diligence Analysis and Risk Assessment
- Systems/Workstations Threats/Controls Risk Assessment
- Social Media Risk Assessment
- Wireless Device/iPad Risk Assessment

Review/Development of Information Security Risk Management Program

As part of the IT Audit, ProBank proposes to perform the following risk assessments that would be provided to the Company in Word format. The risk assessments that would serve to:

1. Identify risks and controls associated with the Company's current Information Technology environment; and

2. Serve as the baseline risk assessment processes that would be maintained by the Company going forward:
   a. Asset-Based Risk Assessment
   b. Distributed Denial of Service
   c. Third-Party Service Provider Risk Assessment
   d. Social Media Risk Assessment

The Systems/Workstations Risk Assessment will identify specific hardware/software components currently used by the Company and should be used as part of the Company's Information Security Program risk management process for the following purposes:

- Maintain data regarding the information and technology assets of the Company, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements;

- Analyze the probability and impact associated with the known threats and vulnerabilities to its assets;

- Identify the strength of industry standard security controls implemented by the Company to protect the Company's network and systems hardware/software components; and

- Recommend processes and/or controls necessary for effective mitigation.

Regulatory Guidance requires the ongoing monitoring of third-party relationships through due diligence processes. The Service Provider Analysis/Risk Assessment will reflect the components required in the initial and ongoing analysis of the company's mission critical service provider, and the results of the analysis process.

The Social Media Security/Compliance Risk Assessment process identifies threats associated with use of Social Media and the processes currently implemented by the Company to mitigate risks associated with Social media.

The objectives of the Wireless Device/iPad Compliance Risk Assessment are to identify risks associated with the use of wireless devices, such as iPads, and to verify controls implemented to mitigate risks associated with the use of such devices is mitigated. The following components were considered in the Wireless Device/iPad Risk Assessment process.

- Unauthorized Access to Data
- Unauthorized Manipulation of Data
- Unauthorized Access to Services
- Misuse of Network Services
- Misuse/Abuse of Privileges
- Lost/Stolen Devices
- Weak Encryption
- Threats Occurring During Transactions
- Unapproved Applications

Business Continuity Plan

ProBank proposes to assist management in updating the Company's Disaster Recovery Business Continuity Plan, which currently includes the following components:

- Risk assessment processes that consider the types of threats with which the Company must be concerned
- Business Impact Analysis that determines the impact of a worse case disaster on the Company's core business services

- Annual testing plans and procedures to verify the validity of the Plan
- Policy and procedures outlining the maintenance of the Plan
- Contingency planning teams and procedures
- Contact names and telephone numbers
- General emergency procedures
- Impact assessment procedures
- Contingency plan initiation procedures
- Alternate site procedures
- Pandemic staffing/processing/testing procedures
- Temporary operating procedures
- Procedures for the production, storage, and retention of back up media

ProBank also proposes to update the Company's Business Continuity Administration Manual; Business Continuity Plan Incident Contingency and Recovery Plan Emergency Procedures Manual; and Information Systems/Security Risk Assessment Manual to:

1. Incorporate changes in the Company environment, and

2. Address new regulatory requirements associated with specific guidance issued for Vendor Oversight, Social Media, Cybersecurity, and Distributed Denial of Service Attacks.

ProBank will meet with the Company's appropriate management and personnel, and gather data required to update the documentation. Upon completion of the fieldwork, ProBank will prepare a draft of the updated Manuals for review by Company management. Upon final approval, ProBank will submit electronic files of the manuals.

Written Report

ProBank will interview Company personnel via conference call for clarification of the Company's procedures and processes, as necessary. Additional questions may be submitted via email to the designated Company contact for the project.

Upon completion of the review/documentation development process, a draft of the Policies and Risk Assessment documentation prepared by ProBank will be submitted to Company management in electronic form for review by the Company. ProBank will make modifications as necessary to the documentation and upon final approval of the documentation by Company management; ProBank will provide the final documentation in "Word" format so the documentation can be updated by the Company in the future.

Part B – Services for Information Technology Audit, Network Vulnerability Testing (Optional), and Social Engineering Testing (Optional)

Information Technology Audit

The scope of the IT Audit performed by ProBank will be based upon Control Objectives for Information and Related Technology (COBIT® 5); Federal Financial Institutions Examination Council's Cybersecurity Tools and the National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity."

COBIT® 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. The COBIT® 5 framework includes the following categories:

- Evaluate, Direct, and Monitor
- Align, Plan, and Organize
- Build, Acquire, and Implement
- Deliver, Service, and Support
- Monitor, Evaluate, and Assess

General control frameworks, such as COSO, Cadbury, CoCo, King III, technical security guidance ISO 17799, and service delivery guidance such as ITIL, are models that emphasize business control and IT Security and Service issues. However, only COBIT attempts to deal with IT-specific control issues from a business perspective. COBIT® 5 aligns with ISO/IEC 38500 "Model for Corporate Governance of IT" through the Evaluate, Direct, and Monitor categories.

The Cybersecurity Controls section of the IT Audit will be based upon the National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity." The NIST framework provides a common language for understanding, managing, and expressing cybersecurity risks both internally and externally. The Critical Security Controls, as identified by the Center for Internet Security will be used as the industry standard technical measure to assess the current security of the Company's technology environment. The Federal Financial Institution Examination Council's (FFIEC) and Information Technology Examination Guidelines are also considered in the IT Auditing Process.

Inherent Risk Profile

ProBank will determine the Company's Inherent Risk Profile as per the FFIEC Cybersecurity Assessment Tool dated June 2015, that identifies activities, services, and products organized in the following categories:

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

The levels range from Least Inherent Risk to Most Inherent Risk and incorporate a wide range of descriptions. The risk levels provide parameters for determining the inherent risk for each category. The most appropriate inherent risk level will be selected for each activity, service, or product within each category.

IT Audit – Governance/Cybersecurity Controls

ProBank will review the Company's IT Policies, Procedures, System documentation, and Controls to obtain reasonable assurance that the Company's IT Governance Process and Cybersecurity Controls meet industry and regulatory baseline standards. Each auditing category will be assigned an "Assessment Rating" that identifies the presence of, or some level of, deficiency in baseline controls. An overall "Assessment Rating" that reflects the comprehensiveness of baseline controls implemented will be assigned. Ratings used in the Assessment Process include the following:

1. Industry/Regulatory Baseline Controls/Processes are implemented.

2. Controls/Processes are informal, limited in scope, and/or not current.

3. Controls are not implemented to address emerging threats within the industry.

4. There is an absence of recognizable control processes and any related procedures.

5. Immediate high-impact security risk to the Company's Customer Information Systems.

The following grid lists work program components included in the ProBank IT Auditing Process.

Information Technology Work Program Components

EVALUATE, DIRECT, AND MONITOR				
Governance Framework	Benefits Delivery	Risk Optimization	Resource Optimization	Stakeholder Transparency
ALIGN, PLAN, AND ORGANIZE				
Manage the IT Management Framework	Manage Strategy	Manage Enterprise Architecture	Manage Innovation	Manage Portfolio
Manage Budget and Costs	Manage Human Resources	Manage Relationships	Manage Service Agreements	Manage Suppliers
Manage Quality	Manage Risk	Manage Security		
BUILD, ACQUIRE, AND IMPLEMENT				
Programs and Projects	Requirements Definition	Solutions Identification and Build	Availability and Capacity	Organizational Change Enablement
Manage Changes	Change Acceptance	Manage Knowledge	Manage Assets	Manage Configuration
DELIVER, SERVICE, AND SUPPORT				
Operations	Service Requests and Incidents	Problems	Business Continuity	Security Services
MONITOR, EVALUATE, AND ASSESS				
Performance and Conformance	System of Internal Control	Compliance with External Requirements		
NIST CYBERSECURITY CONTROLS				
Identify Infrastructure and Threats	**Protect**	**Detect Threats**	**Respond**	**Recover**
Configuration	Firewalls/IDS	Firewall IPS Monitoring	Response Planning	Continuity/Backup
Virtualization	Virus Protection	Internet/Email Communications	Communications/Security	Insurance
Wireless	Internet and Email Content	Network Devices	Analysis	Agreements
Intelligent Peripherals	Patch Management	Activity Monitoring	Mitigation	Communication
Mobile Devices	Access/Authentication	Audit Logs	Improvements	Mitigation
Remote Access	Users/Capabilities	Network Vulnerability Testing		Recovery Planning
Telecommunications-Voice	Encryption	Social Engineering Testing		Cybersecurity Industry Testing
In the Cloud	Physical Security			
Internet Access/E-mail	Cybersecurity Training			
Social Media				
Website				

KEY SYSTEMS				
Core/Deposit Systems	**Loan Platforms**	**Online/Mobile Banking**	**Remote Deposit Capture**	**Wire Transfer**
Systems Overview	System Overview	Systems/Service Lines	Systems Overview	Systems Overview
Communications/Security	Communications/Security	Communications/Security	Communications/Security	Communications/Security
Access/Authentication	Access/Authentication	Multifactor Authentication	Multifactor Authentication	Multifactor Authentication
Users/Capabilities	Users/Capabilities	Monitoring	Monitoring	Monitoring
Monitoring	Monitoring	Customer Training	Customer Training	Agreements
			Agreements	

Cybersecurity Maturity Levels

ProBank will complete the FFIEC Cybersecurity Control Maturity Level exercise to depict the relationship between the Company's Inherent Risk Profile and its domain maturity levels within each of the following five domains:

Domain 1: Cyber Risk Management and Oversight
Domain 2: Threat Intelligence and Collaboration
Domain 3: Cybersecurity Controls
Domain 4: External Dependency Management
Domain 5: Cyber Incident Management and Resilience

Assessment factors and contributing components are described within each domain. Declarative statements are listed under each component that describes an activity that supports the assessment factor at that level of maturity.

- Baseline – Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives.

- Evolving – Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.

- Intermediate – Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk management practices and analysis are integrated into business strategies.

- Advanced – Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of Risk Management Processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.

- Innovative – Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time predictive analytics are tied to automated responses.

IT Auditing Process Key Controls Testing Samples

ProBank will request Company Policies, Procedures, Meeting Minutes, and various system screen prints, systems/network reporting, and other types of information pertaining to the planning, implementation, delivery, security controls, and monitoring of the Company's network and IT Systems. Although there will be many factors that go into the selection of sample sizes, the "Testing Sample Sizes" used in the IT Auditing Process, whenever possible, are listed in the following grid. The sample selection is a common methodology (minimum) used by companies and auditors to test the ongoing effectiveness of controls.

GUIDANCE FOR SAMPLE SIZE SELECTION		
Nature of Control	**Frequency of Performance**	**Minimum Sample Size**
Manual	Many times per day	25
Manual	Daily	25
Manual	Weekly	5
Manual	Monthly	2
Manual	Quarterly	2
Manual	Annually	1
Automated	Test one application of each programmed control activity (*assumes IT General Controls are effective*)	
IT General Controls	Follow the guidance above for manual and programmed aspects of IT General Controls	

Network Vulnerability/Penetration Testing – External and Internal (Optional)

ProBank consultants will attempt to access Company hosts via the Internet from an external "hacker" perspective and identify any discernible vulnerability. Using a Network connection supplied by the Company, ProBank consultants will use specialized vulnerability testing software to identify any internal Network vulnerabilities. ProBank will use Retina Beyond Trust software in the Network Vulnerability/Penetration Testing Processes.

ProBank will test categories of devices for each of the Company's locations separately in order to identify vulnerabilities associated with certain types of devices and/or Company locations. ProBank will review the reports generated through the testing process and prepare a "Network Vulnerability/Penetration Testing Pending Issues/Remediation Status Work Program" that can be used to track the remediation status of each vulnerability configuration security issue identified through the Network Vulnerability/Penetration Testing Processes.

Common categories included in the Network Vulnerability/Penetration Testing Process are listed in the following grid.

Network Vulnerability Testing Components

Network Vulnerability/Penetration Testing Scope

EXTERNAL TESTING					
Configuration	Encryption	Servers	Ports/Protocols	Access	Other Vulnerabilities
INTERNAL TESTING					
Configuration	**Detecting Ops Systems/Services**	**Servers**	**Ports/ Protocols**	**Access**	**Patch Management**
Registry	Database	DNS Servers	Common Ports	Network Policy	Legacy Systems
System Auditing	RPC Services	FTP Servers	Firewall Ports	Accounts	Service Packs
Federal Desktop Stds	NetBIOS	Web Servers	TCP	Admin.	Windows
User Access Rights	DNS Services	Mail Servers	UDP	Users	CISCO
Wireless	Web Applications	SSH Servers	FTP	Passwords	Misc. Software
Windows	Virtualization	SNMP Servers	SNMP	Remote Access	Anti-virus
SSL	Windows Operating Systems	Blackberry	Web Servers		Backup Software
SSH	Internet Protocol		Internet Protocol		Update Services
SNMP	Local UNIX Security Audits		Miscellaneous		
FPT					

Social Engineering Testing (Optional)

Social Engineering Testing (SET) will involve a process in which ProBank sends SET emails to designated Company employees for the purposes of identifying personnel who need additional training on:

- Understanding the threats associated with opening attachments; and
- Responding to email requests submitted from unknown sources.

There will be no customer information involved in the process but the impression will be that additional information will be exchanged at a future time.

All communication used in the SET Process will be approved by the Company's designed IT representative prior to the initiation of the SET Process. The IT representative must also provide the email addresses of employees to which the SET emails are to be sent.

Written Reports

ProBank will provide the IT Audit to the Company's Board of Directors and management following the fieldwork portion of the Audit. The reports will include Audit Findings and Recommendations pertaining to the Company's IT and Information Security Policies, Procedures, and Internal Controls.

Should the Company choose the optional Network Vulnerability/Penetration Testing, ProBank will review all data generated through the testing processes and prepare a Network Vulnerability/Penetration Testing Report, along with the supporting reports generated from Network Vulnerability/Penetration software. Reporting will include a description of each vulnerability, its severity level, and recommendations for mitigating the associated risk.

Upon completion of the optional SET, ProBank will submit a summary report to the Company describing the SET Process and list the email addresses of employees who responded to the SET Process. This information will enable the Company to prepare a training plan for employees as appropriate.

Phase 3 – Consumer Compliance (Lending) Review

This engagement is designed to evaluate the adequacy of the Company's established compliance management program and its ability to ensure technical performance with regulatory compliance matters. At the conclusion of this engagement, ProBank is positioned to provide management with an objective assessment of compliance administration, to identify procedural weaknesses, and to direct attention toward areas posing the greatest risk of regulatory criticism or consumer litigation.

Our consultants examine transactions consummated since the institution's most recent compliance examination, in this case inception. They employ a judgmental sampling process that involves randomly selecting individual files, verifying calculations for those transactions, and reviewing forms for accuracy and timeliness. If we identify a significant number of compliance deficiencies, we may recommend expanding the sample to determine the magnitude of violations.

Following a risk-based approach, we determine the scope and sample size based on several criteria including:

- The volume of loan activity
- New products
- Discussions with the Company's compliance officer

Lending-Related Topics

We anticipate reviewing up to 70 originated and 10 denied transactions (approximately 60 days after first transaction consummation) focusing on the following rules and regulations as well as the Company's internal policies as per the Company's CMP.

- Privacy of Consumer Financial Information ~ Regulation P
- Equal Credit Opportunity Act ~ Regulation B to include complaint processing; thorough Application Review (only relevant for discrimination complaints)
- Fair Credit Reporting Act/FACT Act ~ Regulation V; request to confirm adherence to disputes)
- Truth-in-Lending Act ~ Regulation Z; with an emphasis on closed-end consumer credit, to include pricing and fees from a fair lending perspective, and underwriting considerations
- Electronic Signatures in Global and National Commerce Act
- Unfair, Deceptive, or Abusive Acts or Practices and Regulation AA

- Servicemembers Civil Relief Act (confirmation that customers have not requested to enforce their rights)
- Consumer Protections and Sales of Insurance (as applicable)
- Electronic Funds Transfer ~ Regulation E (as applicable)
- Financial Information Exception for Obtaining and Using Medical Information Policy ~ Regulation FF

Further, this review will include:

- Validation of sustained corrective action to our Phase I identified issues as well as any other applicable internal or external audit findings
- Validation of Compliance Management System and/or program-specific training as addressed within the Company's policies
- Validation of the Company's Third-Party Vendor Management from a due diligence and monitoring perspective

ProBank will provide a written statement regarding the adequacy of the overall status of compliance with applicable rules and regulations. Furthermore, we will assign a significance rating to each recommendation included in the report.

This phase of the engagement may be conducted on-site and/or off-site. Our recommendation is to conduct this phase on-site with increased communications with management and team.

Phase 4 – Bank Secrecy Act/Anti-Money Laundering Independent Review

ProBank proposes to conduct an independent evaluation of the Company's performance with the recordkeeping, reporting, and anti-money laundering responsibilities established under the Bank Secrecy Act /Anti-Money Laundering (BSA/AML) regulations, as well as related regulations established by the Office of Foreign Assets Control (OFAC).

The review will be risk based and include an evaluation of the quality of BSA/AML and OFAC risk management across the company's operations and departments. This assessment will be designed to test the effectiveness of the Company's program to:

1. Provide for a system of internal controls to assure ongoing compliance
2. Provide for independent testing for compliance
3. Designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance
4. Provide training for appropriate personnel

ProBank consultants will use procedures similar to those outlined in the FFIEC's *Bank Secrecy Act/Anti-Money Laundering Examination Manual*. As such, our independent review will include the following:

- An evaluation of the overall integrity and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes.

- A review and critique of the Company's most recent internal BSA/AML risk assessment for reasonableness given the Company's risk profile (products, services, customers, and geographic locations).

- Customer Identification Program (CIP) compliance.

- An evaluation of the adequacy of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) policies, procedures, and processes. Appropriate transactional testing, with particular emphasis on high-risk operations (product and service offerings, customers, and geographic locations) will be performed in determining the effectiveness of CDD and EDD efforts.

- Personnel adherence to BSA/AML policies, procedures, and processes.

- An assessment of training adequacy for BSA, AML, CIP, and OFAC for comprehensiveness, accuracy of the materials, training schedules, and attendance tracking.

- Testing to validate the accuracy and reliability of management information systems (MIS) and other tools used to identify, monitor, and report large currency transactions.

- Testing to verify the Company's adherence to applicable BSA reporting and recordkeeping requirements, including CIP, currency transaction reports (CTRs), CTR exemptions, suspicious activity reports (SARs), funds transfers, and monetary instrument sales.

- As applicable, testing will include an assessment of accuracy and reporting requirements for filing a Report of Foreign Bank and Financial Accounts (FBAR) and Report of International Transportation of Currency or Monetary Instruments (CMIR).

- An evaluation of the effectiveness of actions and efforts to resolve violations and deficiencies noted in previous audits (internal or external) and regulatory examinations.

- An assessment of the adequacy of suspicious activity monitoring processes and procedures to identify unusual activity including, but not limited to, a determination that processes and procedures sufficiently encompass all areas that pose money laundering and terrorist financing risks.

- An assessment of the adequacy of suspicious activity reporting systems including, but not limited to, a review of policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity.

- An assessment of the overall process for identifying and determining whether a SAR is warranted, the process to report suspicious activity including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the Company's practices and policy.

- An assessment of Company's compliance with applicable provisions of the USA PATRIOT Act, including information sharing requirements under Sections 314(a) and 314(b), prohibitions against maintaining correspondent accounts with foreign shell banks, due diligence for correspondent or private banking accounts, and "special measures" requirements.

- An assessment of compliance with Office of Foreign Assets Control (OFAC) screening, blocking, and reporting requirements, as applicable.

- Adherence to the record-retention requirements of 31 CFR Chapter X.

- Compliance with applicable provisions of the Unlawful Internet Gambling Enforcement Act, Regulation GG.

Expanded procedures for products, services, persons, and entities as outlined within the FFIEC *BSA/AML Examination Manual* will be conducted, as applicable to the Company's compliance program.

ProBank will provide a written statement regarding the adequacy of the overall BSA/AML compliance program. Furthermore, we will assign a significance rating to each recommendation included in the report.

This phase of the engagement may be conducted on-site and/or off-site. Our recommendation is to conduct this phase on-site with increased communications with management and team.

Phase 5 – Annual Reviews

On an annual basis, we will validate each of the following:

A. **Compliance Policies** – The Company's compliance policies will be evaluated in line with the scope detailed in Phase 1 of this information packet.

B. **Consumer Compliance (Lending) Review** – We anticipate reviewing up to 70 originated transactions (and a small sample of non-originations) focusing on the rules and regulations, as well as the Company's internal policies per the Company's CMP, as detailed within the scope of Phase 3 of this information packet.

C. **Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Independent Review** – Conduct an independent evaluation consistent with the scope as described in Phase 4 of this information packet.

Phase 5 of the engagement may be conducted on-site and/or off-site. It is recommended Compliance Lending Review and BSA/AML Review be conducted on-site with increased communications with management and team.

ProBank will provide a written statement regarding the adequacy of the overall status of compliance with applicable rules and regulations.

Phase 6 – Fair Lending/Non-Discrimination Analysis

Conduct a fair lending/non-discrimination analysis designed to test the adequacy of the Company's written policies and procedures established to ensure equal treatment for all credit applicants and to determine whether the Company's lending adheres to the principles of fair lending. At the conclusion of this engagement, ProBank will be positioned to provide management and the Board with an objective assessment of the Company's fair lending procedures by comparing application qualifications and outcomes.

Before we begin this analysis, ProBank will conduct a risk assessment designed to help determine the focus and size of analysis to be conducted. When conducting this risk assessment, our consultant will follow guidelines similar to those used by the federal regulatory agencies and will consider:

- The quality of general underwriting guidelines
- The variety, complexity, and introduction of new product offerings
- Growth of specific loan products
- Turnover of key compliance or lending personnel
- Past scheduling and content of fair lending-related training
- Criticisms or recommendations identified during previous regulatory compliance examinations or other applicable internal and external reviews

After completing the initial risk assessment, we will confer with members of the compliance team and management to explain our conclusions and finalize the selection process for the analysis.

It should be understood financial institutions face increasing pressure from regulatory agencies with regard to fair lending. As the regulators have launched renewed efforts with new strategies for detecting potential fair lending violations, a large number of institutions have found themselves having to react to a new level of scrutiny. This renewed focus by the agencies has employed innovative statistical techniques and has imposed considerable time and resource demands on institutions in order to counter allegations of potential disparate treatment. This focus by the agencies also resulted in a number of enforcement actions over the last few years. In addition, fair lending reviews have been expanded to evaluations of consumer credit. An added challenge for consumer lending is the lack of government monitoring information.

Our review will consist of two phases.

During the first phase, we will employ econometric methods to assess differences in pricing practices based on race, gender, and ethnicity. This is done by holding relevant factors "constant" using multivariate regression and testing differences between a single target and control group in each iteration. In the case of pricing, this would be a linear measure, such as differences in the note rate or APR.

The prohibited bases data would be obtained by proxy using methodologies similar to that proposed by the CFPB. This method is known as Bayesian Improved Surname Geocoding or BISG and uses a joint probability assignment using the borrower's surname and the demographic composition of area in which the borrower resides. This analysis will provide an assessment of the overall impact of pricing practices on protected and non-protected groups. Information concerning this approach can be found at:

http://files.consumerfinance.gov/f/201409_cfpb_report_proxy-methodology.pdf

Using the output of the BISG-driven analysis, we will then conduct the non-discrimination analysis of consumer transactions and/or applications; a side-by-side comparison (phase two). We will conduct either an underwriting or terms and conditions comparative analysis; both if statistically possible. The target and control groups to be used will be dependent on the BISG finding but again they will likely be based on race, national origin, sex, or marital status.

The following scenario represents a typical fair lending/non-discrimination side-by-side transactional analysis.

1. During an underwriting analysis (accept/deny), we compare approved loans to control group members to denied applications from the target group. The purpose of the analysis is to determine if loan officers apply consistent underwriting criteria and that exceptions to loan policy for marginal customers are justified, clearly documented, and applied in a non-discriminatory manner.

2. During a terms and conditions analysis, we compare approved loans to members of the control group to approved loans to target group members. The purpose of this analysis is to determine if members of a protected group are offered credit on more burdensome terms (higher rates, higher loan fees, more stringent collateral, or shorter repayment periods) than terms offered the control group.

During this engagement, ProBank also reviews:

- The institution's mission statement with respect to fair lending practices
- The use of overrides or exceptions to Company policy
- Collection policies and practices
- Customer service procedures to determine if applicants are consistently treated courteously and encouraged to complete applications
- The Company's advertising/marketing strategy
- Procedures to respond to consumer complaints and to implement corrective actions associated with regulatory matters

Additional Information and Services

Communication with Management

Our approach is a personal one and we strive to obtain consistent communication between our firm and our clients. Throughout this engagement, your ProBank consultant will be in direct communication with management regarding the progress of the review. We prepare and deliver a report to the Company's CEO, which summarizes the scope of the engagement and includes recommendations for enhancing overall regulatory compliance performance.

ProBank's Experience and Independence

Our company provides such services for clients throughout the country. All engagements are conducted by consultants well versed and experienced in compliance issues and regulatory requirements. Some ProBank consultants are attorneys; however, they do not function as attorneys, and ProBank does not provide legal advice. Our consultants act solely in an advisory capacity and do not perform management functions or make management decisions.

ProBank is independent of our clients and follows a Code of Professional Conduct to ensure ProBank consultants are independent of their financial institution clients. ProBank also complies with all applicable regulatory guidance regarding independence issues.

Protection of Client Customer Information

Pursuant to the Interagency Privacy of Consumer Financial Information Regulations and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, all data and information

relating to our client's customers provided to ProBank, including any non-public personal information ("client customer information"), is treated confidentially and safeguarded by ProBank. ProBank does not disclose or use any such client customer information except as necessary to carry out the services for which ProBank has been engaged, or as required by applicable law.

ProBank safeguards any client customer information through appropriate measures designed to ensure the security and confidentiality of the information; protect against any anticipated threats or hazards to the security or integrity of the information; and protect against unauthorized access or use of the information that could result in substantial harm or inconvenience to a customer.

ProBank employees are held to high standards for maintaining the confidentiality of all information provided by our clients, including client customer information. ProBank employees are instructed to not discuss information provided by our clients with any outside party, and to discuss such information with other ProBank employees only on a bona fide, business-related, need-to-know basis. In addition, ProBank employees are instructed to make every reasonable effort to ensure all confidential client materials and records are kept under proper physical safeguards and are not seen by unauthorized persons.

All client-related paperwork is disposed of through a bonded paper destruction and recycling company, which shreds the paperwork before leaving ProBank's premises. Highly confidential paperwork, including any client customer information, is placed in a locked container to wait shredding.

ProBank uses industry standard hardware and software firewalls to protect its Network and computer systems and the information stored within these resources. To further secure the system, ProBank does not publish the technical information regarding the firewall technology utilized. Internet access through ProBank's firewall is restricted to out-going traffic only. Incoming traffic is limited to specific ports that have been identified within the firewall. ProBank's system also incorporates the use of industry standard workstation and network password restrictions as well as intruder detection lock out mechanisms. ProBank's workstations receive current patches/security updates on a weekly basis, servers on a monthly basis at a minimum. ProBank's system is located in a secured area with access given only to the IT Manager and the Network Administrator. ProBank's website and e-commerce site is located on a separate network, is housed in a different building, and is only accessible via secure connection.

Section III
Commitment and Costs

Corporate Culture

ProBank understands the importance of all our relationships. In particular, we recognize the special trust, faith, and reliance our clients expect and deserve. Our values support our commitment to our clients, our seminar attendees, our employees, and their families.

Our focus is exceptional performance, without equivocation, every seminar, audit, review, or project.

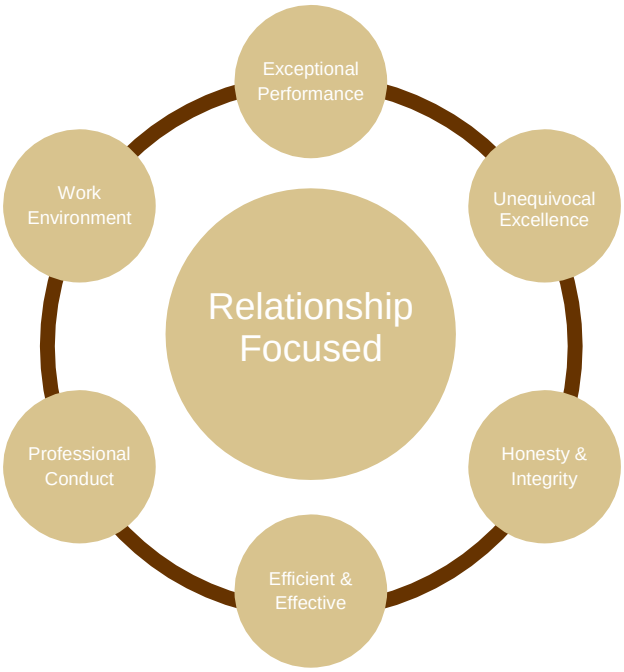
We pursue excellence in all facets, professional knowledge, product delivery (intellectual and otherwise), and interpersonal.

Uncompromising ethics are the foundation of our organization's culture. Independence without conflicts of interest is key to our work and success.

We always look for an efficient, cost-effective approach to accomplish all initiatives. We will be as protective of the client's budget as we are our own.

We focus on professionalism with an expectation of the highest standards of professional conduct. We provide our clients and our employees with the most up-to-date training in their fields of expertise.

As an employee-owned business, we will foster an entrepreneurial environment encouraging creativity, promoting innovation, and valuing quality in all we do. We will not forget the added value a proper work/life balance achieves.



Billing Procedure

Our commitment is to provide the highest quality professional services in the most effective and efficient manner possible. Further, we commit to delivering a valued service for a fair and reasonable fee. We will effectively plan and coordinate with your staff to assure these are fulfilled. Often these services are in coordination with your partnering bank's compliance and/or audit team.

ProBank does not require a retainer for these engagements; however, in certain circumstances, during the initial phases we may require 25% to 50% to be paid up front. ProBank bills monthly; the invoices reflect the fees for professional services, as well as expenses incurred, on behalf of the client during that billing cycle.

In addition to professional fees, reasonable travel and other customary engagement-related expenses are billed to the Company, without upcharge. We use support staff when appropriate, and their costs have been included in the estimates. ProBank expects to operate within the budget guidelines and will only expand the engagement after discussion with, and authorization of the Company's CEO.

Section IV

Our Capabilities to Serve You

Industry Experience

In the later part of 2013, ProBank began educating, consulting, auditing, and advising online lenders. These lenders were referred to us from a traditional bank requesting our expertise. Since that time, we have developed over 25 such relationships which include compliance management program (CMP) policy development, IT/IS audits, transactional reviews for consumer lending, BSA/AML requirements, and a myriad of other topics. Our overarching goal with each lender is to assure their personnel and platform is operating in a compliant manner and producing compliant transactions for the consumer. Frankly, not only is that a regulatory requirement and doing right by the consumer, it is more cost effective for any lender to do their transactions in a compliant manner from the outset. As mentioned previously, we have been providing similar services to the traditional financial industry since 1978.

References

ProBank has produced weeklong compliance schools for various banking associations. For over ten years, our firm acted as a consultant to the FDIC in the development of materials and presentations of its Advanced Consumer Protection, Introduction to Compliance Examination and Community Reinvestment Act schools, and its Consumer Fair Lending and Advanced Fair Lending workshops.

ProBank's seminar experience yields opportunities to provide superior consumer consulting services by professionals who remain at the forefront of the ever-changing regulatory environment. Our seminar and consulting work have a successful track record of over 25 years.

Our consultants conduct hundreds of compliance audits and reviews, on- and off-site each year. Inasmuch as the bulk of our client work is conducted under Non-Disclosure Agreements (NDAs) and often attorney-client privilege, we provide references on request only after appropriate NDAs are in place.

Our Team

To view the entire ProBank Team of professionals please go to https://www.probank.com/about-us.com

Martin (Marty) T. Mitchell, CRCM

Managing Director
Office: 800.523.4778, ext. 258
Direct: 502.479.5258
mmitchell@probank.com

Marty has over 18 years of experience in the regulatory compliance field. After retiring from a successful career as a U.S. Army officer, he served as a Commissioned federal compliance examiner with the Federal Deposit Insurance Corporation (FDIC). As an examiner, Marty was responsible for evaluating a financial institution's compliance with consumer protection laws and regulations as well as conducting Community Reinvestment Act and fair lending examinations for both large and small banks. He also served on a special project at the FDIC's Washington, D. C. headquarters. During his tenure with Capital One, he led the design and implementation of their corporate level mortgage compliance program through a period of business closures, multiple acquisitions, and intense regulatory scrutiny.

As a Senior Consultant with ProBank, Marty served our largest, most complex clients nationwide. For the past six years, he has led our Compliance Consulting Division, speaks on various regulatory topics at seminars and conferences, and continues to serve our financial institution clients coast to coast.

Robert (Bob) J. Mullenbach, CRCM

MPL Relationship Manager, Vice President, and Senior Consultant
Office: 800.523.4778, ext. 250
Direct: 502.479.5250
rmullenbach@probank.com

Bob has over 25 years of experience in the banking industry having worked in the regulatory compliance field for financial institutions across the country. Prior to joining the ProBank team in 2014, Bob served as a Compliance/Community Reinvestment Act (CRA) Officer and Risk Assessment Manager for a large community bank.

Bob serves as our MPL Relationship Manager and has extensive experience conducting consumer compliance reviews for lending, deposit, privacy, and non-deposit investment product regulatory assurance, conducting compliance program risk assessments, and conducting fair lending/non-discrimination analyses. Bob also assists clients with pre-regulatory examination preparation and examination management.

Michael (Mike) O. Anderson, CRCM

Managing Vice President Regulatory Compliance
Office: 800.523.4778, ext. 668
manderson@probank.com

Mike has over 16 years of experience as a banker and consultant in the regulatory compliance and anti-money laundering fields. Prior to joining the ProBank team in 2000, he gained extensive knowledge of all functional areas of banking while working with a large, multi-bank holding company.

Since his time with ProBank, Mike has successfully managed projects with several of our largest clients, including developing and implementing compliance management programs for de-novo financial institutions. He has extensive experience in conducting Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) evaluations in compliance with federal regulatory requirements; conducting consumer compliance reviews for lending, deposit, privacy, and non-deposit investment product regulatory assurance; conducting BSA/AML and compliance program risk assessments; and conducting fair lending/non-discrimination analyses. Mike also assists clients with pre-regulatory examination preparation and examination management.

K. Natalie Straus, J.D., CRCM

Vice President and Senior Consultant
Office: 800.523.4778, ext. 268
Direct: 502.479.5268
nstraus@probank.com

Since joining the ProBank team in 2011, Natalie has been involved in performing regulatory compliance reviews and frequently speaks at numerous conferences, seminars, webinars, and school on a variety of regulatory compliance topics.

She has extensive experience conducting consumer compliance reviews for lending, deposit, privacy, and non-deposit investment products regulatory assurance and fair lending/non-discrimination analysis.

Lisa C. Brock, CCBIA
Senior Consultant
Office: 800.523.4778, ext. 408
lbrock@probank.com

Lisa has over 20 years of experience in the banking industry, having worked in the lending, accounting, operations, compliance, and internal audit areas of banking. Before joining the ProBank team in 2009, she worked as the Internal Auditor and Compliance Officer for a community bank where she completed a broad range of both internal and compliance audits.

Lisa has expertise conducting Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) evaluations in compliance with regulatory requirements and conducting reviews for lending, deposit, and privacy regulatory assurance. She also has extensive experience performing independent validation testing of BSA/AML automated surveillance and monitoring programs.

Darla J. Brogan, CISA, AAP, CRISC
Senior Consultant
Office: 800.523.4778, ext. 251
Direct: 502.479.2251
dbrogan@probank.com

Darla has over 30 years of banking experience, specializing in technology and operations. She is qualified in banking operations, loan servicing, and customer service operations, data processing systems, cash management, and state-of-the-art technologies for electronic presentment.

Darla brings with her expertise in a myriad of areas including:

- Information Technology Audits
- Network Vulnerability Testing (NVT)
- Social Engineering Testing (SET)
- Information Security Program Development or Auditing
- Identity Theft Program/FACT Act Program

- Development or Auditing
- Automated Clearing House (ACH) Audits
- Risk Assessment Documentation/Analysis
- Data Processing Vendor/Systems Analysis and Implementation
- Technology Vendor Oversight Policy and Procedure Development or Auditing
- Deposit/Retail/Loan Operational Analysis in comparison to Industry Best Practice Systems Processes and Workflow Procedures
- Electronic Banking Best Practice Analysis
- Disaster Recovery/Business Resumption Planning and/or Testing
- Information Technology Strategic Planning
- Expert Witness in Matters of Bank Operations, Electronic Banking, and Information Technology Best Practices

Douglas (Doug) L. Bushman, CRCM

Senior Consultant
Office: 800.523.4778, ext. 413
dbushman@probank.com

Doug has over 20 years of experience in the financial industry, having worked in the regulatory compliance field and as a business trainer for financial institutions across the country.

His expertise includes evaluating compliance management programs and assisting with development and or program enhancement. He has extensive experience conducting compliance reviews for lending regulatory assurance and conducting fair lending/non-discrimination analyses. Doug also assists clients with pre-regulatory examination preparation and examination management.

Kathleen A. Caldwell, J.D., CAMS

Senior Consultant
Office: 800.523.4778, ext. 245
Direct: 502.479.2245
kcaldwell@probank.com

Kathleen joined the ProBank team in 2003, and works exclusively assisting financial institutions with their Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) compliance programs. Her expertise includes all aspects of BSA and AML compliance program management, as well

as performing independent validation testing of BSA/AML automated surveillance and monitoring programs. Her clients include both community banks, large multi-bank holding companies with a national presence, as well as numerous MPLs.

Michelle Spelbring

Consultant
Office: 800.523.4778, ext. 415
mspelbring@probank.com

Michelle has over 18 years of experience in the financial industry, having worked in the regulatory compliance field and as a business trainer for financial institutions across the country.

Her expertise includes evaluating compliance management programs and assisting with development and/or program enhancement. She has extensive experience conducting compliance reviews for lending regulatory assurance and conducting fair lending/non-discrimination analyses. Michelle also assists clients with pre-regulatory examination preparation and examination management.

Karen I. Mannix

Consultant
Office: 800.523.4778, ext. 416
kmannix@probank.com

Karen is a consultant with ProBank. Prior to joining the firm in 2016, she worked for a large billion dollar financial institution with positions of Branch Manager, Compliance Trainer, and Business Policy Senior Analyst. Karen has 20 years of experience in the financial industry. At ProBank, she is part of the Marketplace Lending Team working with clients and conducting reviews for policy, lending compliance and CMS, and BSA/AML.


E • PLURIBUS • UNUM
LIBERTY
ProBank
Austin