COASTAL
COMMUNITY BANK®

ONLINE AND MOBILE BANKING POLICY

Reviewed November 2021
Approved by the Board of Directors December 2021

ONLINE BANKING POLICY

Background and Purpose

The term Online Banking refers to any type of service or product that enables a customer to perform banking activities and transactions from non-branch locations using public network facilities.

The Board of Directors (Board) and management of Coastal Community Bank (Bank) recognize that Online Banking presents unique risks and challenges that are not present in traditional banking products and services. The Board acknowledges that documented Online Banking Policies are necessary to protect the interests of the Bank and its customers.

While Online Banking has quickly become recognized as an important step in banking delivery systems for customers, there are certain risks inherent with any delivery system. Potential causes of a system compromise include natural disasters, system attacks, and participant failures. The Bank accordingly must evaluate not only its level of risk, but also its ability to manage that risk.

The purpose of this policy is to designate responsibilities and help guide the Bank's management and personnel in proper procedures, risk management, internal controls and other issues related to Online Banking.

Responsibilities

Board of Directors

The Board of Directors of Coastal Community Bank (Board) has ultimate responsibility for the electronic systems employed by the Bank. The Board's approval is required for technology strategic plans and major technology expenditures including feasibility studies and risk assessments.

Board approval is also required for significant changes or updates to the Online Banking Policy.

eBanking Department

The eBanking Department is responsible to review and report on levels of transaction activity and report potential risks and issues of significance to the Executive Management of the Bank.

The eBanking Manager has been designated to act as the Online Banking Coordinator. This individual has a working knowledge and understanding of the elements of Online Banking and related electronic funds transfer issues.

The eBanking Department is responsible to:

1. Review transaction, security and account activity reports on a daily basis.
2. Review the levels of customer activity and potential effects on system performance.
3. Ensure that internal controls are reviewed and enhanced, as necessary, to prevent financial loss or improper disclosure of confidential information.
4. Ensure the ongoing management of risk.
5. Manage the bank's online banking services.
6. Provide and promote cash management services to business clients.
7. Keep informed about new technological developments, potential capability enhancements and potential new risks.
8. Work closely with the IT and Audit/Compliance Departments to communicate and implement necessary actions across product lines and departments.

Online Banking Risk Assessment

Risk management is the ongoing process of identifying, measuring, monitoring and managing potential risk exposure. A risk management program is critical to identifying and responding to any incident. The Bank's evaluation will be designed to be commensurate with the complexity and sophistication of the Bank's Online Banking activity and encompasses all significant operational, legal and reputation risk areas. The monitoring of risk throughout the Bank will be an ongoing process.

The online environment introduces aspects to traditional risk management such as transaction speed, geographic reach and user anonymity. A primary focus of risk management is to minimize the negative effects of a problem situation. This can be particularly difficult in an environment that offers speed, sophistication, and access to many users.

The Bank will identify and assess potential risks to Online Banking activity and will determine the appropriate compensating controls for prevention, detection and standards to be maintained for each of the potential risks identified. This risk assessment will include sections regarding Strategic Risks, Transactional/Operations Risks, Compliance/Legal Risks, Reputation Risk, Liquidity and Market Risks, and Credit Risks. The Bank will, on an annual basis, perform an Online Banking Risk Assessment and revise and report to the board to document any problems and review emerging trends.

Online Banking Objectives

The Bank has chosen to offer Online Banking products and services in order to achieve the following objectives:

1. Retain and expand the Bank's current consumer/retail customer base.
2. Retain and expand the Bank's current business customer base.
3. Reduce current and future transaction and overhead costs.

Online Banking Services

Coastal Community Bank will offer Online Banking services for consumers and businesses, as well as Cash Management services for qualified businesses.

The Online Banking Services offered to consumers and businesses are as follows:

- Deposit account balances and history inquires
- Loan inquiries
- Export account history
- View statements
- Internal transfers between eligible Coastal Community Bank accounts
- Item stop payment requests
- Check reorder (via Main Street, a third-party vendor)
- Initiation of address change
- Bill payment
- Secure e-mail to the bank
- Mobile Banking
- Mobile Photo Deposit
- Person to Person Payments and Requests (Zelle – consumer only)

In addition to the above, the following services are available to qualified Cash Management customers:

- Wire transfer requests
- Automated Clearing House (ACH) payments and receipts
- Tax payments
- Positive Pay Services
- Remote Deposit Capture (Coastal Remote Deposit)

Customers must have an existing deposit relationship with Coastal Community Bank before they are allowed to establish an online banking relationship.

New deposit or loan applications are NOT offered on the Bank's website through Online Banking at this time.

Description of Network and Processing Environment

Background

FIS, a third-party data processor, provides core data processing, item processing, online banking, mobile banking and bill pay services for the Bank.

Transaction and Data Flows

Online banking internal transfers between transaction accounts are performed by FIS in real-time and require no action from a Bank employee. Loan payments and draws are processed automatically at nightly processing. All cash management transactions are system automated and forwarded to the appropriate systems of record for regular processing.

Throughout the day, account activity is displayed online real-time to include memo-posted transactions through teller activity at the branch level as well as POS/ATM activity.

The processing of online bill payments is completed via ACH or by check processing and requires no action from a Bank employee.

System Security

Responsibilities

The eBanking Department is responsible for all Online Banking related security matters including the monitoring, review and follow-up of all security issues related to the suite of Online Banking products.

The eBanking Department is responsible to:

- Review security reports and activity logs for both employees and customer activity on a daily basis.
- Ensure that there is no deviation from the security and password requirements contained in this policy.
- Review transaction activity reports for unusual transactions on a daily basis.
- Research and respond to fraudulent activity warnings and suspended transaction alerts generated by FIS.
- Report suspicious activity to the Bank's Security Officer

Customer Security Requirements

Note: Customers are required to have an existing deposit relationship before they are allowed to establish an online banking relationship.

The Coastal Community Bank website includes a comprehensive education section for customer consumption that includes Security and Fraud Prevention for eBanking and mobile products and services.

Security requirements for Online Banking are:

1. All users must have usernames between 3 and 30 characters in length and encrypted passwords that are at least 8 characters in length.
2. New accounts and existing customer accounts requiring password resets are directed to go through an out-of-band password reset feature of the online banking system. If a manual

password must be assigned, customers are given a temporary password that requires a change upon first login to the system.

3. The Mobile Banking platform allows password resets, however the end user must pass multi-factor authentication in order to complete the process..
4. Retail customers will be allowed access to only those accounts for which they are signatories. Commercial accounts may have users who are not signatories; however, a signatory on the applicable account must approve these users.
5. The Online Banking systems utilize out-of-band authentication, which requires the user to receive either a phone call or text containing a passcode to gain access to the system.
6. The Mobile Banking system uses out-of-band authentication, which requires the user to receive either a phone call or text containing a passcode to first gain access to the system.
7. Consumers may enroll for the Zelle product via the mobile app. Only mobile phone numbers that are currently listed within the Bank's core banking system will be allowed for enrollment.
8. The Bank requires each Cash Management customer to designate at least one "Company Admin" user of the system. That individual is then responsible to designate which accounts to open to non-admin users, what services will be available to each non-admin user and under what limitations (if any). The Bank does not control or oversee the Company Admin function. Customer contractually agrees that all action taken by the Company Admin, or any person designated by the Company Admin is authorized, and all such persons are agents for purposes of use of the Cash Management system. Persons executing agreements related to the Cash Management system must be a corporate officer or other person who has the authority to enter into an agreement with the Bank. The person or persons authorized to act as Company Admin will be assigned on the enrollment (or change) form.
9. Cash Management transactions, such as wire transfers or ACH originations are approved individually by bank employees, following either an out of band transactional confirmation within the system or by a separate, confirmed contact with the customer outside of the online banking system.
10. Consumers logging into Online and Mobile Banking for the first time must accept the disclosure as displayed in the system. Within this disclosure is information outlining the customer's responsibility for the confidentiality and security of their passwords.
11. Corporate/Business customers will sign all applicable agreements for Cash Management Services and will also be provided with a disclosure which outlines responsibility for the confidentiality and security of their passwords.
12. Customer software is required to support 128-bit encryption to protect confidential data when it is transmitted to the customer from Online Banking.
13. Four unsuccessful attempts to sign on to Online Banking will result in an automatic lockout from the system. Access, after lockout, may only be restored by a bank employee.

Employee Security Requirements

Only employees with a legitimate business need will be granted access to the Digital Administration Tool, the FIS application allowing administrative access to the Online Banking platforms to perform administrative functions. Administrative functions include setup of new enrollments, account maintenance, password changes, access to bill payment, Zelle and any other necessary customer support functions. Bank employees that are authorized to access the Digital Administration Tool are required to have a User ID and password issued by an administrator of the system.Employee password requirements are that they:

1. Must be at least 8 characters in length with uppercase/lowercase letters, numbers and at least one symbol.
2. Are case sensitive.
3. Must not be disclosed to any other person.

Other System Security Measures

1. Customers are able to request access to the system due to a forgotten password by successfully passing out-of-band authentication.
2. Bank personnel may assign new temporary passwords that are required to be changed upon first sign-on to Online Banking.
3. Bank personnel cannot view customer passwords.
4. Online Banking sessions will automatically be terminated after 15 minutes of inactivity by the customer.
5. Passwords are encrypted in transport and in storage.
6. Data is provided in TLS 1.2 security protocol end to end throughout a customer's session.

Mobile Banking

Mobile and wireless banking occurs when a customer accesses the Bank's networks through cellular phones, tablets and personal digital assistants (or similar devices) via telecommunication companies' wireless networks or Wi-Fi connections. While wireless services can extend the reach and enhance the convenience of banking products and services, wireless communications currently have certain limitations that tend to increase the risks associated with this delivery channel. Therefore, it will be the policy of the Bank to recognize and manage the risk inherent in mobile and wireless banking.

Risk Implications

Mobile banking services can significantly increase the Bank's level of transaction/operations and strategic risks.

Transaction/Operations Risk

Wireless services create a heightened level of potential operations risk due to limitations in wireless technology. Security solutions that work in wired networks must be modified for application in a wireless environment. The transfer of information from a wired to a wireless environment can create additional risks to the integrity and confidentiality of the information exchanged.

Strategic Risk

The Bank has carefully evaluated the significant strategic risks posed by this service delivery channel. Standards for wireless communication are still evolving, creating considerable uncertainty regarding the scalability of existing wireless products. As a result, extra diligence was used in preparing and evaluating the cost-effectiveness of investments in wireless technology.

Risk Management

Risk management of wireless-based technology solutions, although similar to other electronic delivery channels, may involve unique challenges created by the current state of wireless services and wireless devices. The Bank will utilize the various risk management strategies detailed below:

Encryption of wireless banking activities is essential because wireless communications can be recorded and replayed to obtain information. Encryption of wireless communications can occur in the banking application, as part of the data transmission process, or both.

Transactions encrypted in the banking application (e.g., financial institution-developed for a mobile device) remain encrypted until decrypted by the Bank. This level of encryption is unaffected by the data transmission encryption process.

Wireless encryption that occurs as part of the data transmission process is based upon the device's operating system. A key risk-management control point in wireless banking occurs at the wireless gateway-server where a transaction is converted from a wireless standard to a TLS protocol and vice versa. Wireless network security reviews focus on how the institution establishes, maintains, and tests the security of systems throughout the transmission process, from the wireless device to the Institutions' systems and back again.

The Bank will ensure effective controls are in place to reduce security vulnerabilities and protect data being transmitted and stored.

Password Security

Mobile banking increases the potential for unauthorized use due to the limited availability of authentication controls on wireless devices and higher likelihood that the device may be lost or stolen. This creates the risk that authentication credentials can be easily observed or recalled from a device's stored memory for unauthorized use. As technology progresses the Institution will implement the latest standards (as defined by industry experts) in regard to passwords and authentication. Per the Mobile Banking Terms and Conditions document agreed to by each customer upon download of the application, all mobile devices must be password-protected if the CCB Mobile Application is installed on the device.

Product and Service Availability

Wireless communication "dead zones" - geographic locations where users cannot access wireless systems - expose the Institution and its service providers to reliability and availability problems in some parts of the U.S. and other countries. For some areas, the communication dead zones may make wireless banking an unreliable delivery system. Consequently, some customers may view the Institution as responsible for unreliable wireless banking services provided by third parties. The Institution's role in delivering wireless banking includes developing ways to receive and process wireless device requests. The Bank will inform wireless banking customers that they may encounter telecommunication difficulties that will not allow them to use the wireless banking products and services.

Disclosures

The Bank will ensure that the products offered in its mobile banking offering will allow for delivery of required disclosures, otherwise those products and/or services will not be allowed to be accessed via mobile banking.

Operational Procedures

Detailed operating procedures are maintained in separate documents for Online Banking, Mobile Banking, Cash Management and ACH processing.

Operational Controls

The Bank's operational controls include the following:

1. Separation/Segregation of Duties.
2. Review of daily reports including the Admin Activity Report.
3. Ongoing reconciliation of Control and Settlement accounts
4. Retention of all appropriate transaction and processing records.
5. Periodic audit review of reports and transaction activity.

Insurance

Bank has a Financial Institution Bond that covers Coastal Community Bank's Online Banking activities.

Audit

Audit procedures and separation of duties are required to have consistent and effective controls. Audit programs are designed to protect the interests of the Bank and its consumers.

Compliance

Before proceeding with any new Online Banking product or service, or any major changes to the existing products or services, the legal and regulatory issues must be evaluated. The eBanking Department is responsible to ensure that approvals are obtained from Senior Management prior to implementation.

Online Banking may or may not fall within certain guidelines for paper transactions.

The Bank will be compliant with any and all regulations that may apply to Online Banking products.

The Bank's Compliance Officer will be responsible for implementing and monitoring Online Banking compliance.

The Risk Management Department will complete the monthly Online Banking Checklist. Other areas that will be reviewed as appropriate to determine if they are affected by laws, regulations or other regulatory guidance:

1. Advertising
2. Disclosures/Notices
3. Applications
4. Record Keeping

Online Banking Privacy Policy

The Board recognizes the responsibility of the institution and its employees to safeguard the financial records and personal information of the institution's customers. Various state and federal acts, laws and regulations govern the customer's right to privacy. Furthermore, failure to maintain a customer's confidential information can result in civil lawsuits and/or loss of reputation.

Vendors and Outsourcing

The Bank may rely upon vendors, third-party support or other outsourcing considerations. Online Banking vendors are evaluated as follows:

1. Ability of the vendor to provide the level of service required.
2. System documentation, user training and ongoing support.
3. Financial condition.
4. Identification of the risks and accountability for both the vendor and the Bank.
5. Assessment of the vendor's ability to manage risk, internal controls, system security, etc.
6. Review most recent third-party audits of the vendor.
7. Maintenance agreements.
8. Current and available insurance coverage to mitigate risk.
9. Disaster recovery support.
10. Contingency alternatives.
11. Ability to provide support for compliance issues.
12. Ability to safeguard personal information of Bank's customers.

Disaster Recovery Contingency Plans

A disaster will be declared when one or more Online Banking services normally offered by the Bank becomes or is in jeopardy of becoming unavailable. The most common disaster is a malfunction of online banking hardware or software.

A disaster can also occur as a result of flooding, fire, tornado nuclear attack, sabotage, riot, power failure, etc. These types of disasters will almost certainly affect other data processing systems of the Bank as well. These other systems will usually be considered more critical than the online banking system, and, as such, will be addressed more promptly. Refer to Coastal Community Bank's Disaster Recovery Plan for more information.