ELECTRONIC BANKING POLICY

11.21.2022| Responsible Party: Director of Branch Banking

Table of Contents

Policy Overview

It is the policy of Community First Bank (CFB) to provide clients with a variety of electronic banking services. In summary, this policy covers the following operational areas:

- Wire Transfers
- Client Originated Transactions
    - ACH Origination via cash management (commercial online banking)
    - Mobile and Remote Deposit Capture "RDC" (virtual deposits of client checks accepted for services rendered)
    - Merchant Card Services (debit and/or credit card acceptance for services rendered)
    - X937 file processing originated using client systems
- Internet Banking
- Lockbox

It is not the policy of the Bank to provide any of these services to non-clients. Wire requests from non-clients require the approval of the authorized ACH approval authority (CEO, COO, CFO, CLO, or Director of Branch Banking).

The Board acknowledges that a special Electronic Banking Policy is necessary to protect the interests of the institution and its clients. This policy is designed to help guide institution personnel (including the Board) in proper procedures, internal controls and other items related to Electronic Banking services.

Risk Assessment

The Board of Directors of Community First Bank understands that Electronic Banking Transactions involve risk. Because of this, prior to implementing these types of transactions, the authorized ACH approval authority will identify and assess the risks (legal, compliance, reputation, credit, market, liquidity, and operational) associated with each activity.

Therefore, the Board directs management to implement controls and procedures that will mitigate these and other risks to the extent possible while providing efficient service to our clients. In addition, we will include regulatory guidance when assessing this delivery system, such as the interagency guidance on risk management of remote deposit capture (see Interagency Statements, Risk Management of Remote Deposit Capture 1/09), the FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual and appropriate booklets contained in the FFIEC Information Technology Examination Handbook.

The board appoints the Director of Branch Banking to be primarily responsible for the Electronic Banking Policy. The policy further directs the Audit Committee to include the areas covered by this policy in the Annual Internal Audit Relative Risk Assessment.

The complexity of the risk identification and assessment process will vary depending on the scope of exposures faced by our institution.

Legal and Compliance Risks

Management also needs to identify and assess exposure to legal and compliance risks related to Electronic Banking areas. For each clearing method, we need to consider applicable legal and regulatory requirements, such as timing and amount of funds availability, as well as the time frames for handling returned items. We should also assess our agreements to verify that liability is allocated appropriately and that other matters, such as methods for resolving disputes and choice of legal jurisdiction, are addressed adequately.

Finally, we should evaluate potential risks and regulatory requirements under Bank Secrecy Act laws and regulations when designing and implementing Electronic Banking solutions. We should assess to what extent we could be exposed to the risk of money laundering activities as well as our ability to comply with anti-money laundering laws and regulations and suspicious activity monitoring.

Operational Risks

Management should understand operational risks and ensure that appropriate policies, procedures and other controls are in place to mitigate them, including physical and logical access controls over Electronic Banking systems (i.e. Fedline system, merchant card terminals, original deposit items at client locations, online banking systems, electronic files and retained nonpublic personal information). Management should also assess carefully how Electronic Banking affects existing risks and implement mitigating controls.

Electronic Banking services located at a client's location expose our institution to operational risks at the point of usage. These risks can be unique to each client's location and information security systems. For example:

- Faulty equipment, inadequate procedures or inadequate training of clients and their employees can lead to inappropriate document processing, poor image quality and inaccurate electronic data. Ineffective controls at the client location may lead to the intentional or unintentional alteration of deposit item information, resubmission of an electronic file or redeposit of physical items.
- Inadequate separation of duties at a client location can afford an individual end-to-end access to the processes and the ability to alter logical and physical information without detection. In the typical RDC process, original deposit items are not submitted to the financial institution but are retained by the client or the client's service provider. Therefore, it is important for us to require clients to implement appropriate document management procedures to ensure the safety and integrity of deposited items from the time of receipt until the time of destruction or other voiding.
- Depending on the type of systems implemented, information security risks may extend to our own internal networks and networks of our service providers. These technology-related operational risks include failure to maintain compatible and integrated IT systems between our institution, service providers and the client. For example, a client or service provider may modify RDC software or hardware or fail to update or patch an associated operating system in a timely manner.
- There also may be risks related to Web application vulnerabilities, authentication of a client to the systems and encryption used at any point in the process.

We also need to consider the authentication method appropriate for each system our client's use. As stated in the Interagency Guidance on Authentication in an Internet Banking Environment, the FFIEC agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to client information or the movement of funds to other parties. Accordingly, business client's utilizing ACH origination as well as wire functionality within our business online banking product will require the usage of a secondary token authentication.

In addition, certain aspects of fraud risk are elevated in an electronic banking environment.

- Check alteration, including making unwarranted changes to the Magnetic Ink Character Recognition (MICR) line on the image of scanned items, may be more difficult to detect when deposited items are received through RDC and are not inspected by a qualified person.
- Forged or missing endorsements, which may be detected in person, may be less easily detected in an RDC environment.
- Certain check security features may be lost or the physical alteration of a deposited check – such as by "washing" or other alteration techniques – may be obscured in imaging or electronic conversion processes.
- Counterfeit items may also be difficult to detect.
- Duplicate presentment of checks and images to our institution represents both a business process risk and a fraud risk.
- The potential for insider fraud may be greater with RDC because we typically do not perform background checks on our clients' employees who may have access to physical deposit items or electronic files.
- Access by clients and their staff to nonpublic personal information contained on, or represented by, deposit items may also increase the risk of identity theft.

Unauthorized access to online banking platforms by either client employees or hackers. This unauthorized access could result in funds being embezzled from the client's checking accounts via any electronic banking platform. In response to this risk, management requires that any business client allowed to originate transaction out of their account electronically are required to utilize a token for authentication means. To help prevent fraudulent transfers, the token password will be in put a second time when clients process their outgoing file.

Risk Management Mitigation and Controls

If a comprehensive risk assessment supports a management conclusion that the risks associated with the various Electronic Banking solutions can be effectively mitigated, measured and monitored, management should implement appropriate risk management policies. These policies should establish risk tolerance levels, internal procedures and controls, risk transfer mechanisms where appropriate and available and well-designed contracts that meet our risk management needs.

Client Due Diligence and Suitability

The risks associated with Electronic Banking solutions generally warrants greater client selectivity than the risks associated with traditional deposit services. Management should establish appropriate risk-based guidelines to qualify clients for this service. In general, information gathered while conducting client identification and client due diligence procedures as part of our BSA/AML program can support the assessment of client suitability.

In addition:

- For new and existing clients, a suitability review should involve consideration of the client's business activities, risk management processes, geographic location and client base.
- The depth of such review should be commensurate with the level of risk.
- When the level of risk warrants, our staff should include visits to the client's physical location as part of the suitability review. During these visits, our staff should evaluate management, operational controls, risk management practices, staffing, the need for training and ongoing support, and the IT infrastructure.
- Our staff should review available reports of independent audits performed at the client location related to IT, RDC and associated operational processes. When appropriate, based on risk, we may choose to rely on self-assessments by our RDC clients when these address the controls and risk management practices that would otherwise be reviewed during on-site visits by our staff.

The resulting conclusion from this due diligence may result on caps being placed on client dollar volumes processed on a daily, weekly or monthly basis. Said limits will be communicated to clients once established.

Vendor Due Diligence and Suitability

If we rely on service providers for all Electronic Banking activities, we need to ensure implementation of sound vendor management processes (see the Bank's Vendor Management Procedures).

Training for Clients

Management will ensure that clients receive sufficient training for the Electronic Banking Solutions that clients utilize. Sound training should include documentation that addresses routine operations and procedures, including those related to the risk of duplicate presentment and to problem resolution.

Contracts and Agreements

Strong, well-constructed contracts and client agreements are critical in mitigating our risks.

- A third party documents provider develops contracts and agreements with other financial institutions that accept checks in the form of electronic files, with third-party service providers and with clients that participate in any electronic banking process.
- Contracts and agreements should be appropriate for our specific environment and should identify clearly each party's roles, responsibilities and liabilities.
- Agreements should establish the control requirements identified during the risk assessment process and the consequences of noncompliance.

The contracts should cover risks and responsibilities relative to the physical equipment used by the client. Specific contract provisions for consideration include the following:

- Roles and responsibilities of the parties, including those related to the sale or lease of equipment and software needed.
- Handling and record retention procedures for the information in RDC, including physical and logical security expectations for access, transmission, storage and disposal of deposit items containing nonpublic personal information.
- Types of items or transactions that may be transmitted.
- Processes and procedures that the client must follow, including those related to image quality.

- Imaged documents (or original documents, if available) RDC clients must provide to facilitate investigations related to unusual transactions or poor-quality transmissions, or to resolve disputes.
- Periodic audits of the processes, including the IT infrastructure.
- Performance standards for our institution and the client.
- Allocation of liability, warranties, indemnification and dispute resolution.
- Funds availability, collateral and collected funds requirements.
- Governing laws, regulations and rules.
- Our authority to mandate specific internal controls at the client's locations, audit client operations or request additional client information.
- Our authority to terminate the RDC relationship.

Business Continuity

Management will also ensure that we have the ability to recover and resume electronic banking operations to meet client service requirements when an unexpected disruption occurs. Therefore, our business continuity plan must address electronic banking systems and business processes, and the testing activities should assess whether restoration of systems and processes meets recovery objectives and time frames. To the extent possible, contingency plan development and testing should be coordinated with clients using electronic banking products.

Other Mitigation and Control Considerations

Management will also implement, as appropriate, other controls that mitigate the operational risks of electronic banking products.

- These controls should be designed and implemented to ensure the security and integrity of nonpublic personal information throughout the transmission flow and while in storage.
- Separation of duties or other compensating controls at both the institution and the client location can mitigate the risk of one person having responsibility for end-to-end processing.
- Strong change control processes coordinated between the institution and client can help to ensure synchronized platforms, operating systems and applications, and business processes.

- To reduce the risk of items being processed more than once, deposit items can be endorsed, franked or otherwise noted as already processed. When insurance coverage is available and cost effective, we may be able to mitigate risk further.

Risk Management: Measuring and Monitoring

Management will develop and implement risk measuring and monitoring systems for effective oversight of electronic banking activities and ensure that clients using these solutions have implemented operational and risk monitoring processes appropriate to our choice of technology.

Transactions can be accepted up to 30 days prior to the effective date.