Treasury Management Security Procedures (Schedule B)

Type	Category	Description	Can be waived
Mandatory	Login Authentication	WesBanco uses step up Out of Band authentication to a mobile phone or with a token at the time of login. Over time the system learns your behavior, so the OOBA is only generated if a step-up is needed for reasons such as a changed IP address, login from different devices, or changed security settings.	No
	Passwords	WesBanco mandates complex passwords involving 8-12 characters, special characters and non-repeating characters.	No
	Company ID	In addition to a username and password, all companies are issued a Company ID that must be used at login. The Company ID is not based on any publicly available information.	No
	Alerts	Several alerts are configured at the bank level and are not able to be removed by the Client. These alerts primarily relate to changes to user profiles or other administrative items.	No
	Transaction Dual Control	WesBanco will mandate dual control on all Wire and ACH transactions that are deemed to be high risk. A client may opt to configure dual control on other internal transactions as well.	Yes w/ approval and execution of specific waiver
	Transaction OOBA	WesBanco requires the use of OOBA for every Wire and ACH transaction. This applies to the transmission only, so in the case of Dual Control, the OOBA is sent only to the approver.	No
	Electronic Transactions Call-Backs	Due to the high risk nature of Wire and ACH Transfers, WesBanco runs a system to identify potentially fraudulent wire transfers. If an Electronic Wire Transfer triggers a fraud alert, the Fraud Department may reach out to the Client to verify the authenticity of the transaction.	Yes w/ approval and execution of specific waiver
	One Time Codes	Due to the risk of account takeover, if our Customer Service Center is unable to fully identify a caller; or the caller is requesting a higher risk action such as a limit increase; we may ask the Client to retrieve and properly provide a systemically generated one time code.	No
	Positive Pay Exception Item Default Rule	For clients using Positive Pay, a systemic Exception Item Default Rule as defined in Section V.10 of the Master Agreement will take effect for any un-decisioned items. Effective 10/1/2023; WesBanco mandates this rule to reject transactions.	Yes
	Company Limits	WesBanco establishes limits for Wires, ACH, and Remote Deposit Capture for all clients. For additional information on limits and limit overrides, reference Section II of the master agreement.	No
Strongly Recommended	Administrative Dual Control	WesBanco strongly Recommends establishing dual control on administrative changes in addition to Wire and ACH. This ensures that any changes to users including permission changes, additions, and deletions will require two individuals to complete.	N/A
	Separation of Duties	WesBanco strongly recommends establishing an administrative role that is not responsible for entering or approving financial transactions.	N/A
	Additional Alerts	In addition to WesBanco defined alerts, the Client has the ability to configure myriad other alerts triggered by different actions. Client should review optional alerts and enable those that are relevant to their organization.	N/A
	User Limits	WesBanco strongly recommends setting individual limits on system users in addition to the Company Limits referenced above. This allows the Client to limit the transactional risk of any user within the organization.	N/A
	Client Initiation of all Electronic Transfers via CashFlow Connect	For any ACH or Wire Transactions initiated by the Client, WesBanco strongly recommends upload of all files for such transactions be done using the CashFlow Connect business online banking environment.	Yes w/ approval for use of SFTP

Best Practices for Security

1. **Verify Recipient Information:** Double-check the recipient's name, account number, and bank details before initiating the wire transfer. Any errors could lead to funds being sent to the wrong account. Do not accept Wire instructions via email. Always call, verify, and speak with the receiver.
2. **Use Secure Networks:** Only initiate wire transfers from a secure and trusted network. Avoid using public Wi-Fi or shared computers, as they may expose your sensitive information to potential hackers.
3. **Keep Credentials Confidential:** Never share your online banking login credentials, wire transfer details, or security codes with anyone. Your bank will never ask for security codes or passwords via email or phone.
4. **Be Cautious of Phishing Attempts:** Beware of phishing emails, messages, or calls pretending to be from your bank. Always verify the receiver's identity and never click on suspicious links or provide personal information.
5. **Regularly Monitor Account Activity:** Keep a close eye on your account for any unusual transactions or unauthorized wire transfers. Report any suspicious activity to your bank immediately. Alerts will be sent to your email and show up in online banking.
6. **Use Verified Contacts:** When communicating with your bank regarding wire transfers, use verified contact information from their official website or statements.
7. **Be Wary of Urgent Requests:** Be cautious of urgent or last-minute wire transfer requests, especially if they come from unexpected sources. Scammers often create a sense of urgency to pressure you into making hasty decisions.
8. **Secure Your Devices:** Ensure that your devices are protected with up-to-date antivirus software and operating system patches to prevent malware attacks.
9. **Keep a Record:** Maintain a record of all wire transfer details, including transaction receipts and confirmation numbers, for future reference.
10. **Regularly Update Contact Information:** Keep your contact details updated with the bank to ensure you receive notifications about account activity promptly.
11. **Use Encrypted Communication:** If you need to send sensitive information to your bank, use secure and encrypted communication channels like secure messaging through online banking.
12. **Be Skeptical of Unsolicited Offers:** Be cautious of unsolicited offers or deals that require wire transfers. Verify the legitimacy of such offers and receivers via phone before proceeding. Do not accept email communication as verification.
13. **Contact Your Bank Immediately:** If you suspect any fraudulent activity or unauthorized wire transfers, contact your bank immediately to block further transactions and initiate necessary investigations.