ACH ORIGINATOR
FRAUD PREVENTION REFERENCE GUIDE

A practical reference for ACH Originators to protect against fraud, email compromise, account takeover, and unauthorized ACH activity.

The Importance of ACH Fraud Prevention

ACH fraud poses a significant threat to businesses of all sizes, potentially leading to financial losses, reputational damage, and even legal consequences. Fraudsters often impersonate trusted vendors, employees, executives, or financial institutions and create urgency to pressure staff into changing payment instructions or moving funds.

The strongest defenses are consistent procedures and internal controls.

1. **Always Verify.** Confirm every new or changed payment instruction using a trusted phone number already on file. Never use the number supplied in the request.
2. **Dual Control.** Separate responsibilities in payment creation, approval, and release authority. Require additional approval for high-risk, unusual, or high-dollar payments.
3. **Review Daily.** Investigate unfamiliar company names, payees, amounts and account changes immediately.

Vendor and Payment Change Verification

1. Call the vendor or payee using a trusted phone number already on file.
2. Confirm that the request is legitimate.
3. Verify all payment details, including the account and routing numbers.
4. Document the verification according to your organization's procedures.
5. Obtain any required secondary approval before making the change.

ACH File Filtering Services

ACH file filtering service is a stop payment/block of all ACH files on a business account. The business client provides the bank with a listing of approved/authorized ACH companies. This approved listing is added to the client's ACH file filtering service as exceptions. When an ACH transaction is attempting to clear the client's account, it is compared against the listing of all approved/authorized ACH companies. Should the ACH transaction be from a non-approved company, the business client is notified and is asked to review the ACH transaction item for authentication.

Employee Awareness

To protect your organization, please inform your employees of the following fraud prevention practices and warning signs:

- SFB team members may contact you about services or account activity, but they will not call to ask for your online banking password, security token, or one-time authentication code.
- Nacha will not ask for your online banking credentials or ACH file data. Treat unsolicited calls claiming otherwise as suspicious.
- Caller ID, display names, and email addresses can be spoofed. Use a trusted number and make an independent outbound call.
- Do not click unexpected links or open unexpected attachments. Navigate to known websites directly.

Cybersecurity Safeguards

ACH originators should consider implementing the following cybersecurity safeguards to protect their data:

- Use multi-factor authentication and unique user IDs.
- Keep operating systems, browsers, and security tools up to date.
- Originate payments over a secure network, not a public Wi-Fi network.

Incident Response

If you suspect fraud or unauthorized activity, take the following actions:

1. **Call SFB.** Contact our Treasury Management Team and identify the transaction, amount, date, receiving information, and why it is suspicious.
2. **Secure access.** Disable or reset compromised credentials, revoke sessions, change passwords from a known-clean device, and review multi-factor authenticator methods.
3. **Preserve evidence.** Save original messages, logs, and approval records.
4. **Notify internal teams.** Notify appropriate members of leadership and the IT department.

Contact Information

Direct treasury management support and service questions to treasurysupport@sfbank.com. In case of an emergency, our Treasury Management Team will coordinate with the appropriate SFB departments to respond to the situation and determine the next steps.