

ACH Origination Fraud Prevention Information

Please distribute this document to all applicable users for fraud prevention guidance.

Common Fraud Techniques and Mitigation Strategies:

Common Fraud Techniques	Mitigation Strategies
- Vendor impersonation fraud is a scheme in which fraudsters pose as known partners and instruct companies to change legitimate ACH payment information to fraudulent account information. - Payroll diversion fraud occurs when a criminal tricks a company's HR or payroll team into changing legitimate direct deposit information to fraudulent direct deposit information. - Authorized Push Payment (APP) fraud occurs when scammers manipulate victims into authorizing a real-time transfer of funds to a fraudulent account. - Business Email Compromise (BEC) occurs when an attacker mimics or hijacks legitimate business email accounts to misdirect payments.	- Segregation of duties – Require multiple employees to review changes to payment information. - Confirm independently – Call the vendor using a known, trusted phone number. - Verify requests – Establish a mandatory verification process for changes to direct deposit information. - Require Authorization Forms – Require a specific Authorization Form for direct deposit requests. - Stop and verify – Call the person or organization requesting the payment. - Question urgency – Be suspicious of requests that demand an immediate response. - Employee training – Train staff to recognize signs of phishing; verify sender email addresses; and verify change requests via a known method.

Fraud Prevention Best Practices:

Focus on high-risk scenarios: A significant amount of fraud involves changing account details to reroute payments. Exercise extreme caution when processing any request to alter account information.

The steps below are best practices when a Receiver (Payee) requests changes to their ACH information.

1. Authenticate the requestor when adding or updating a Receiver (payee).
2. Confirm any change request through a separate channel using known contact information. (HIGHLY recommended.)
3. Verify the account number of the Receiver prior to the first payment. (Consider using Prenotification Entries.)
4. Verify the routing number of the Receiver prior to the first payment.
5. Confirm the effective date of the transaction(s).
6. Confirm payment-related information.
7. Confirm sufficient funds in the funding account.
8. Obtain approval for the transaction (such as an ACH Authorization Form).
9. Initiate the transaction.
10. Require a **second person** to confirm and release the transaction. (This is referred to as “dual control.”)
 - a. **NOTE:** While FCB does not currently require dual control ACH Origination, it is HIGHLY recommended. If you do not currently utilize this process, contact us to find out more information.

For More Information:

For more information regarding ACH Origination cybersecurity and fraud prevention, NACHA provides a free “Protecting Against Cyber Fraud” booklet that is available here: [**"Protecting Against Cyber Fraud"**](#)