Responding to Suspected Supplier Payment Fraud

PURPOSE

Prompt action is critical when fraudulent supplier payment activity is suspected. This Quick Reference Guide outlines initial actions agencies should consider while coordinating with OSC and other appropriate parties.

Agency-specific procedures should also be followed.

AGENCY IMMEDIATE ACTIONS

Notify Appropriate Personnel

Immediately notify appropriate agency management and financial leadership.
If applicable, notify your agency’s information security personnel and legal counsel in accordance with agency procedures.

- Notify your supervisor and agency financial leadership immediately.
- Notify your agency Information Security Office if email compromise or phishing is suspected.
- Do not process any additional supplier payment requests until the situation has been evaluated.

Contact OSC & Provide Key Information

Notify OSC as soon as possible after identifying suspected fraudulent activity. Early notification may improve the ability to evaluate available recovery options and begin appropriate follow-up activities.

Please email the OSC Contact Center at ncfspaymentfraud@ncosc.gov and copy the NCFS ePay mailbox at ncfsepay@ncosc.gov.

Information to be prepared to provide:

- Supplier Name
- Supplier Number
- Agency Name

- Agency Contact Information
- Payment Amount
- Payment Date
- Date banking information was changed if known
- Bank account information involved if known
- Copies of the banking change request if available
- Correspondence with the supplier
- Any verification documentation if collected
- Any other supporting documentation
- Additional information may be requested as the review progresses.

OSC IMMEDIATE ACTIONS

Contact Agency to Gather Key Details

The Data Maintenance team will reach out to the agency contact to collect the details available about the fraudulent payment. NCFS Management will also be notified. The DM analyst will gather internal information about the supplier including:

- Payment request form and supporting bank documentation
- Security Verification Question responses
- Phone Verification details
- Date of the payment setup or change
- All email communications about the payment request

Inactivate the Payment Information

The Data Maintenance team will add an end date to the payment record to inactivate the suspected fraud site. The analyst will also check other supplier sites for the fraudulent information and inactivate those sites as well.

Notify Other Teams

Ensure the Statewide Accounting team is notified of the fraudulent payment. The Central Compliance Team will contact Bank of America as soon as possible to request confirmation that the payment has cleared the bank account. If payment has not cleared the account Bank of America may attempt to perform an ACH Reversal or ACH Deletion. Neither action is guaranteed to be successful if the receiving bank or account holder has already received or withdrawn the funds. Central Compliance will then reach out to DST as soon as possible. OSC, Bank of America, and DST will coordinate efforts to locate and recover the funds.

FREQUENTLY ASKED QUESTIONS

What should I do first?

Notify agency management and OSC immediately. Time is an important factor when evaluating available response options. Do not delete emails or alter documentation while the incident is being evaluated.

Can the payment be recovered? Or can a payment be recalled or reversed or stopped?

Recovery depends on several factors, including…

- How quickly the bank is notified
- Whether the funds have been withdrawn
- The payment method
- Coordination between the agency, OSC, and financial institutions

Should I contact the supplier?

Yes. Independently verify the request using a trusted phone number or contact information already on file. Do not rely on the email address or phone number contained in the suspicious request.

Who should contact the bank?

The supplier should contact their bank if the fraudulent payment was made to that institution. OSC will contact Bank of America for electronic payments.

Should law enforcement/SBI be notified? Or maybe a broader question – who will coordinate the responses to external parties?

Agencies should follow their established incident response procedures. Additional guidance may be provided based on the circumstances.

Should I contact my agency's insurance company?

Yes, the agency should contact their insurance company once all details about the incident are available.

Will payments stop to this supplier?

Electronic payments will stop for this supplier until the incident is resolved.

How will agencies be notified if they didn’t identify or know of the fraudulent activity?

OSC will notify the agency if they are not aware of the fraudulent activity.

IMPORTANT: Before Processing any Supplier Banking Change:

- Independently verify the request.
- Use trusted contact information already on file.
- Document the verification.
- Escalate suspicious activity immediately.
- When in doubt, stop and verify before processing.

Last Updated

Mon, 09/14/2026
Printable PDF