Best Practices for Supplier Payment and Banking Information Setup & Changes (Agency Perspective)

Purpose

The NC Office of the State Controller (OSC) continues to evaluate opportunities to strengthen payment security and reduce the risk of fraudulent supplier payment activity. While OSC processes supplier payment information within NCFS, agencies serve an important role in validating requests received from suppliers before they are submitted to OSC.

This document provides recommended practices for agencies when suppliers request payment or banking information changes. These recommendations are intended to complement existing agency internal controls and support a consistent statewide approach to safeguarding State funds.

Recommended Practices

Supplier Requests Payment or Banking Changes

When a supplier contacts your agency requesting changes to payment or banking information, take extra care to verify the request before taking any action. Fraudsters often impersonate legitimate suppliers or compromise supplier email accounts in an attempt to redirect payments.

Recommended Practices

- Do not complete or submit supplier setup forms or provide supplier banking information on behalf of the supplier. Suppliers should independently complete and submit all required ePay enrollment or banking change forms.
- Carefully review the request for potential fraud indicators, including:
  - Misspelled names or unusual grammar.
  - Changes to the supplier’s email address, phone number, or other contact information.
  - Emails sent from a different domain or an address that closely resembles the supplier’s legitimate email.
  - Missing or altered email signatures.
  - Requests that create sense of urgency or ask to bypass normal procedures.
  - Requests to communicate only by email or to avoid phone verification.

- Be cautious about the information you provide to suppliers. While invoice numbers, purchase order numbers or check reference numbers can be discussed freely, avoid sharing banking account information or other sensitive information that could be used to facilitate fraud or answer OSC's banking verification forms.
- Watch for common fraud scenarios, such as:
  - An individual asks agency staff to assist with completing supplier setup or banking change forms for OSC in order to obtain the necessary information to complete these forms.
  - Bank letters or supporting documentation appear altered or inconsistent
  - Requests are made shortly before a large payment is expected.

If anything about the request appears unusual or inconsistent, stop and independently verify the supplier before proceeding further.

Independently Verify Supplier Requests

Independent verification is one of the most effective controls for reducing the risk of fraudulent payment or banking changes. If suppliers reach out to agencies, both the agency and OSC have responsibilities within the supplier payment process to independently verify requests before payment information is established or modified.

Requests to establish or change supplier payment or banking information should never rely solely on an email, written request or supporting documentation provided with the request. Verification should be performed using trusted information that was obtained independently of the request.

Recommended Practices

- Verify request using trusted contact information already maintained by your agency or obtained from an independent source, such as:
  - Existing supplier records (Sub W9 or NCFS Supplier Record)
  - Previous contract or procurement records
  - The supplier's official website
  - Previously established points of contact
- Do not rely on contact information within the request itself, including:
  - Phone numbers listed in the email
  - Email signatures
  - Contact information in PDF attachments or supporting documentation in the request
  - Recently changed contact information that has not been independently verified
- Contact the supplier using a trusted phone number and confirm:
  - The individual requesting the change Is authorized to act on behalf of the supplier
  - The supplier initiated the request
  - The requested banking information is accurate

    - The supplier understands the requested change and expects it to occur
- Document the verification performed in accordance with your agency's internal policies and procedures. Maintaining sufficient documentation supports agency internal controls, provides an audit trail, and assists with any follow-up questions or investigations. Recommended documentation to keep may include:
    - Date and time the verification was performed
    - Name and title of the individual contacted
    - Method of verification (e.g., phone call, established point of contact)
    - Name of the agency employe performing the verification
    - Summary of the verification performed and outcome
    - Any supporting documentation retained in accordance with agencies policies

Note: Independent verification should occur outside the original communication that initiated the request. Fraudsters frequently compromise legitimate email accounts or create convincing fraudulent documentation. Contacting the supplier through an independently verified communication channel significantly reduces the risk of business email compromise and payment diversion fraud.

Enhanced Verification Considerations

State agencies vary significantly in size, transaction volume, payment activity, and operational complexity. As a result, agencies should establish verification procedures that are appropriate for their operations and overall risk profile. The examples below represent recommended best practices that agencies may consider when evaluating and strengthening their supplier verification procedures.

The following matrix provides examples of enhanced verification procedures for higher risk supplier requests.

Request	Recommended Verification
New Supplier Setup	Independent Phone Verification
Banking Information Changes	Phone Verification and review of supporting documentation
High-dollar (payments over $5,000) or critical suppliers	Supervisor Review + Phone Verification
Requests submitted after normal business hours or identified as urgent	Additional review and management approval

Suggested Talking Points for Supplier Verification Calls

The following are examples of suggested talking points that agencies may use when independently verifying supplier payment or banking information. These examples are intended to support a professional and consistent verification process and may be modified to fit the agency's specific circumstances.

Before contacting the supplier, review the guidance in this section to ensure you are using trusted contact information, following your agency's verification procedures, and avoiding the disclosure of sensitive information during the conversation.

- Opening the Conversation:
  - As part of the State's payment security procedures, we independently verify requests involving supplier payment or banking information. These verification steps are designed to help protect both your organization and the State from increasingly sophisticated payment fraud.

- Confirming the request:
  - We're calling to confirm that your organization submitted a request to establish or change payment or banking information and that the request is legitimate.

- Confirming the authorized representative:
  - Can you confirm that you are authorized to request changes to your organization's payment or banking information? If not, could you direct us to the appropriate individual?

- Verifying the information:
  - To protect your organization's information, we'd like you to confirm the information included in your request so we can verify its accuracy before processing the change.

- If the supplier is unaware of the request:
  - Thank you for letting us know. We will not process the requested change at this time. We recommend that your organization review this matter internally, as it may indicate unauthorized activity or a compromised email account. Once you've had an opportunity to investigate, please contact us using your organization's established point of contact.

- If the supplier questions the call:
  - We understand and appreciate your caution. As part of our payment security procedures, we're independently verifying this request to help protect both your organization and the State from payment fraud. If you're more comfortable, you may end this call and contact our office using the publicly available phone number listed on our agency's website or through your established agency point of contact.
  - We encourage suppliers to independently verify our identity before discussing payment or banking information. We would rather delay processing a request than have either party disclose information without confidence that they are speaking with the correct individual.

- Closing the conversation:
  - Thank you for helping us verify this request. These verification procedures are an important part of protecting both suppliers and the State from payment fraud

Verification Tip: Avoid using leading questions or disclosing sensitive information during the verification process. Rather than asking, “Is your new account ending in 4321?” ask the supplier to provide or confirm the requested information. This approach strengthens the verification process by confirming the supplier’s identity without unintentionally revealing information that could be used to facilitate fraud.

Responding to Suspected Fraud or Supplier Compromise

If an agency believes supplier’s payment or banking information may have been compromised, promptly follow the agency’s incident response procedures and notify the appropriate internal and external parties. Early notification and communication can help limit additional fraudulent activity and improve the likelihood of recovering funds.

Internal Notifications:

- Information Security
- Finance Team (Manager)
- Internal Audit
- Agency Leadership

External Notifications:

- OSC (ncfspaymentfraud@ncosc.gov)
- DST (CBS.help@nctreasurer.gov)
- SBI - (www.ncsbi.gov/Divisions/Misuse-of-State-Property)

Agencies should also notify the supplier using a trusted point of contact and encourage the supplier to contact its local law enforcement and financial institution immediately to determine whether additional accounts or transactions may have been affected.

Refer to the Responding to Suspected Supplier Payment Fraud web page for recommended response actions, notification procedures, and recovery considerations.

Cyber Incident Response Plan

Each agency should have a cyber incident response plan in place that includes internal procedures related to payments and potential fraud. This plan should be reviewed annually for accuracy and completeness.

Additional information on cyber incident response plan requirements can be found on the NCDIT webpage (external link).

Conclusion

Payment fraud continues to evolve, requiring agencies to remain vigilant and periodically evaluate their internal controls and verification procedures. While no single control can eliminate all risk, implementing layered controls, independently verifying supplier requests, and following established procedures can significantly reduce the likelihood of fraudulent payment activity.

These recommended practices are intended to supplement—not replace— each agency’s existing policies, internal controls, and applicable State requirements. Agencies should adapt these recommendations as appropriate, based on the size and complexity of their operations, transaction volume, payment activity, and overall risk profile.

Last Updated

Wed, 09/23/2026
Printable PDF