

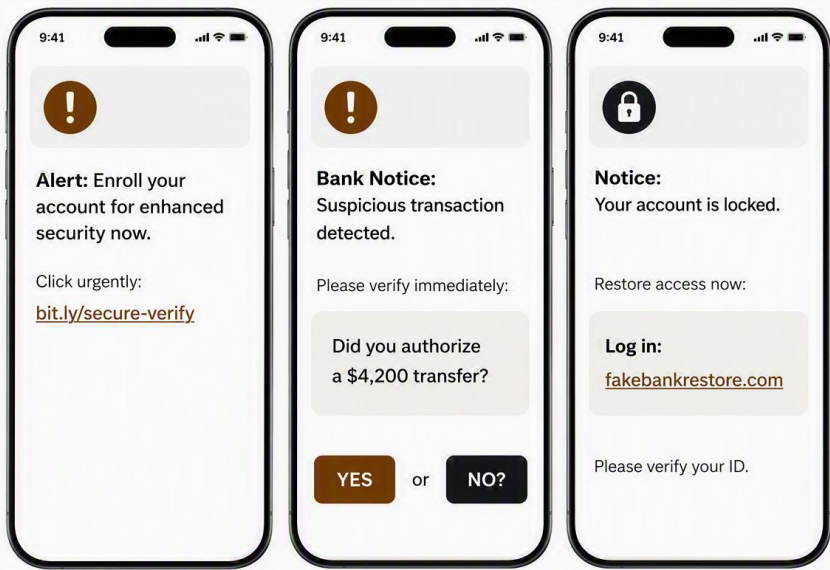
The trust trap: smishing

Payment controls that help spot familiar-looking fraud before funds move.

!

Scenario: Security verification required

At the end of a busy workday, Sarah receives a text that appears to come from her bank asking all wire and ACH users to activate additional authentication. She replies “YES,” follows a link to a professional-looking login page and enters her credentials. A caller then claims to be from the bank’s security team, references the enrollment in progress and asks for the one-time passcode (OTP). Sarah provides it. The text, website and call are fraudulent, giving the attackers both her credentials and a live authentication code to access the account and attempt fraudulent transactions.



Examples of messages that should trigger independent verification.

Anatomy of the scam

- 1

Fraudulent Text
Urgent security alert appears to come from the bank.
- 2

Spoofed Website
Victim clicks the link and enters credentials.
- 3

MFA Request
Fraudster obtains an OTP or approval from victim, posing as bank representative.
- 4

Account Access
Criminal gains access to the platform.

Stop when a request...

- Arrives by unsolicited text asking you to enroll, verify or reactivate access.
- Directs you to open a link and enter bank credentials.
- Is followed by a caller claiming to see your activity or enrollment.
- Asks for an OTP, token code or other authentication secret.
- Instructs you to enter unfamiliar keypad commands during a call.

Common schemes

- Spoofed bank texts claim that urgent security enrollment is required.
- Phishing sites imitate the bank's branding and login experience.
- Fraudsters call during the fake enrollment to appear credible and helpful.
- Captured credentials and a live token code are used to access the account.

Control mindset

- Navigate directly to the known bank website or application.
- Never disclose a one-time passcode or token code.
- Verify requests using official contact information already on file.
- Report suspicious texts, emails, websites and calls according to your company's security procedures.

Don’t fall into the trust trap. Reminder to keep an eye out for:

Urgent Link

Unfamiliar Shortened URL

Request for Credentials or One-Time Code

Controls to protect authentication workflows

Build these controls into routine access and incident-response processes.

Control	What to do
Trusted access paths	Implement controls that limit access to financial platforms through approved channels, such as known bank websites, saved bookmarks, and official applications, rather than links delivered by text or email.
Passcode confidentiality	Establish and reinforce a clear policy that one-time passcodes, token codes, and authentication prompts must never be shared with anyone, including individuals claiming to represent a bank or technology support. The policy should apply to all employees, regardless of role, seniority, or authority.
Independent verification	Verify unsolicited enrollment, security or account-access messages through trusted contact information already on file or the secure message center within the official platform.
Reporting and escalation	Encourage quick reporting of suspicious texts, websites and calls through established internal channels so the organization can take timely action.

Remember these potential red flags

- ✓ Does the request appear urgent?
- ✓ Was the request/message unsolicited?
- ✓ Does the request appear to come from an authority? (your bank, CEO, business partner or legal firm)
- ✓ Is the person claiming a transaction is fraud or that access to your account will be locked?

What questions would a J.P. Morgan employee ask?

- How were the payment instructions received?
- Who validated the payment instructions?
- Was a callback performed to validate the payment?

If you have any doubts or suspicions:

- Terminate the call.
- Call the JPMC Fraud Hotline (866-619-3053).
- Call your Relationship Team.

BONUS GUIDE FOR YOUR PAYMENTS TEAMS

The trust trap: Acquisition

Payments controls that help spot familiar-looking fraud before funds move.

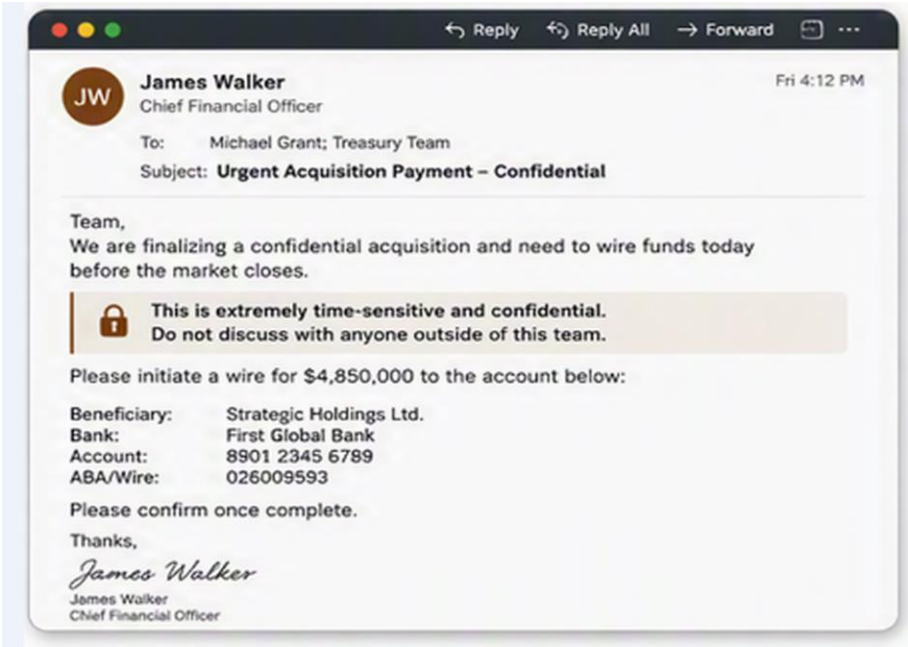


Scenario: The confidential acquisition

A Payment Operations specialist receives an email that appears to come from the CFO of a major client. The message states that a confidential acquisition is underway and an urgent wire transfer is needed to complete the transaction. The employee is instructed not to discuss the request with anyone else.

A follow-up call from someone claiming to be the client's attorney reinforces the request, provides payment instructions and stresses that timing is critical.

The communications appear legitimate, but both the email and phone call are fraudulent. The attack is designed to exploit authority, urgency and confidentiality while discouraging independent verification.



How the scheme unfolds

- 1 Executive impersonation**
Fraudsters spoof a legitimate executive to create authority.
- 2 Attorney follow-up**
A second call reinforces legitimacy and provides details.
- 3 Urgency and secrecy**
Pressure and confidentiality discourage verification.
- 4 Fraudulent payment**
Funds are directed to a criminal-controlled account.



Stop when a request...

- Comes from a senior executive or key client.
- Requires immediate payment.
- Uses confidentiality to limit discussion.
- Includes unusual payment instructions.
- Comes from external channels



How the scheme works

- Executive email creates authority.
- Fraudster follows with a phone call.
- Pressure reduces scrutiny.
- New instructions bypass normal procedures.



Control mindset

- Always verify independently.
- Mandate dual authorization.
- Don't deviate from approval procedures.
- Escalate unusual requests via approved internal channels.
- Always confirm information through internal channels.

Don't fall into the trust trap. Reminder to keep an eye out for:

Authority	Urgency	Confidentiality	New instructions
-----------	---------	-----------------	------------------

Controls that could prevent this

Strengthen processes to reduce the risk of fraudulent wire requests.

Control	What to do
 Dual authorization	Implement dual authorization for all wire and ACH payments as well as for any administrative changes within banking platforms.
 Approved channels	Prohibit approval requests through email, text or voicemail alone. Reinforce this policy and train employees to escalate if they notice any deviation.
 Independent verification	Independently verify payment requests with an outbound call using a known phone number from company records. Do not rely on inbound calls or contact information directly from the requestor.
 Urgent-request procedures	Establish clear procedures for handling urgent or confidential payment requests. Instill trust in your team but always verify the proper protocol was taken.
 Beneficiary Information Governance	Monitor changes in beneficiary details or addition of new accounts. Notify other coworkers about the changes to prevent a transaction from going to a fraudulent destination.

**Key takeaway**

Impersonation fraud often targets processes, not technology. When employees consistently follow verification and approval procedures, even highly convincing requests from executives, clients or attorneys can be stopped before funds are lost.

Before approval, ask:

☐ Is the request expected and consistent with normal business activity?

☐ Were payment instructions verified through a trusted, independent channel?

☐ Did the request follow approval and segregation-of-duty requirements?

☐ Are urgency, secrecy, new contact details or channel changes resolved before release?

Remember these potential red flags

- ✓ Does the request appear urgent?
- ✓ Was the request/message unsolicited?
- ✓ Does the request appear to come from an authority? (your bank, CEO, business partner or legal firm)

BONUS GUIDE FOR PAYMENTS TEAMS

The trust trap: C-suite impersonation

Payment controls that help spot familiar-looking fraud before funds move.

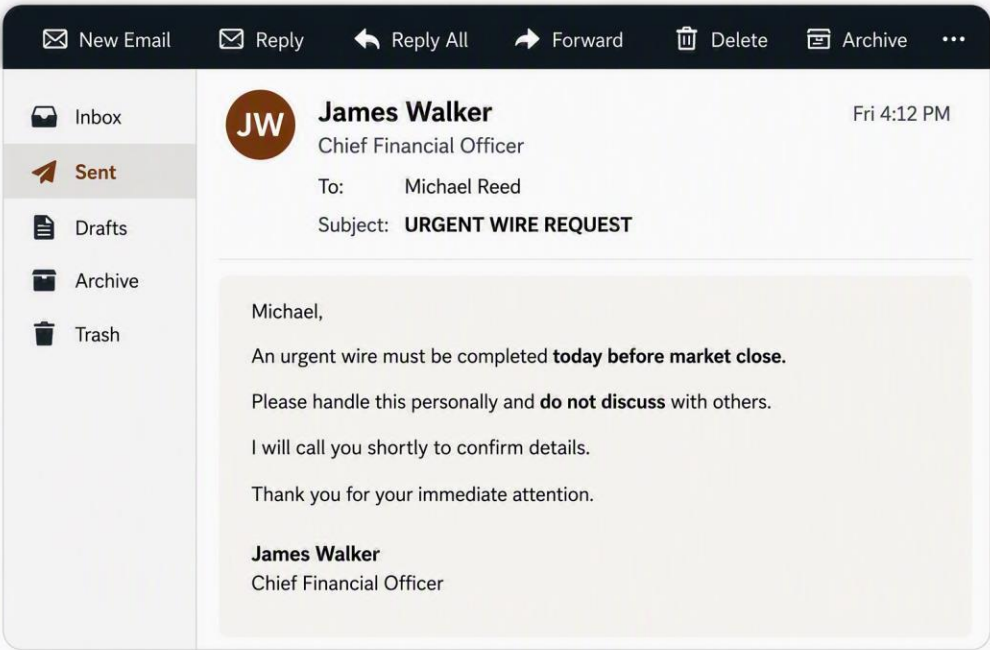
!

Scenario: The urgent executive payment request

Late Friday afternoon, Michael, a Treasury analyst, receives an email that appears to come from his CFO requesting an urgent wire transfer before a deadline. The message uses the executive's name, signature and writing style.

A follow-up call appears to come from the executive's office, reinforcing the request and increasing pressure to act quickly.

Believing the request is legitimate, Michael bypasses normal approval procedures and releases the payment. The email and call were fraudulent, and the funds are transferred to a criminal-controlled account.



Attack progression

- 1

Executive email
Fraudsters spoof a legitimate executive to create authority.
- 2

Spoofed phone call
A call appears to come from the executive office, reinforcing urgency and legitimacy.
- 3

Approval bypass
Pressure, secrecy and a market-close deadline led to bypassing normal review.
- 4

Fraudulent payment
Funds are released to a criminal-controlled account.

Stop when a request...

- Claims to come from a senior executive.
- Requires unusual urgency
- Uses confidentiality to discourage normal review.
- Asks you to bypass the established approval process.

Fraud signals

- Senior executive request that's out of pattern with normal work processes
- Unusual urgency
- Confidentiality
- Request to bypass process
- An unformatted or unofficial email signature (i.e., sent from personal phone)

Control mindset

- Require dual approval for every wire and ACH payment.
- Never rely on email, text, voicemail or caller ID alone.
- Verify through a known number in company records and through proper company channels.
- Escalate urgent, confidential or unusual payment requests.

Don't fall into the trust trap. Reminder to keep an eye out for:

Executive identity

Urgent deadline

Spoofed caller ID

Approval bypass

Controls that could prevent this

Strengthen processes to reduce the risk of fraudulent wire requests.

Control	What to do
 Dual approval	Require dual approval for all wire and ACH payments, as well as administrative changes within your platform.
 Approved channels	Prohibit approval requests through email, text, or voicemail alone. Enforce a policy of company communication only through approved company channels
 Independent verification	Independently verify requests using a known phone number from company records.
 Urgent-request procedures	Establish clear procedures for handling urgent or confidential payment requests and create a culture that values employees who speak up about irregularities.
 Beneficiary Information Governance	Monitor changes in beneficiary details or addition of new accounts. Notify other coworkers about the changes to prevent a transaction from going to a fraudulent destination.



Payments Team takeaway

A request can come from a real organization and still be fraudulent. When money is moving or payment details are changing, familiarity should never replace verification.

Before approval, ask:

- | | |
|---|--|
| ☐ Is the request expected and consistent with normal business activity? | ☐ Did the request follow approval and segregation-of-duty requirements? |
| ☐ Were payment instructions verified through a trusted, independent channel? | ☐ Are urgency, secrecy, new contact details or channel changes resolved before release? |
| | ☐ Has an exception been escalated for review? |

Remember these potential red flags

- ✓ Does the request appear urgent?
- ✓ Was the request/message unsolicited?
- ✓ Does the request appear to come from an authority? (your bank, CEO, business partner or legal firm)