SCENARIO 2 | FINANCE, PROFESSIONAL SERVICES, REAL ESTATE, ANY BUSINESS THAT SENDS PAYMENTS

Business Email Compromise and Wire Fraud

A vendor's email account is compromised and used to redirect a large payment to a fraudulent bank account.

Suggested length	60 to 90 minutes	**NIST CSF 2.0 functions**	Protect, Detect, Respond

Exercise objectives

- Test payment verification and bank-change procedures
- Practice rapid bank recall and law enforcement reporting
- Identify mailbox compromise indicators and containment steps

Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

#	When	What happens
1	**Tuesday, 2:15 p.m.**	Accounts payable receives an email from a long-time supplier with new bank details and an urgent request to pay a $186,000 invoice before Friday.
2	**Thursday, 10:00 a.m.**	The payment was sent on Wednesday. The real supplier calls asking why their invoice is unpaid.
3	**Thursday, 11:30 a.m.**	IT finds an inbox rule in your controller's mailbox that moves all messages from the supplier to an obscure folder, created from an unfamiliar overseas IP address.

Discussion questions by role

Role	Questions
Finance / CFO	• How fast can our bank initiate a recall? • Who verified the bank change, and how?
IT Lead / MSP	• How did the attacker get into the controller's mailbox, and what else could they read?
Legal / Privacy Counsel	• Does the mailbox contain personal data that triggers notification?

Role	Questions
Executive Sponsor	• Who bears the loss, and do we need to involve the supplier's insurer?
Everyone	• What information do we need that we do not have? • Who outside the company must we contact, and do we have their numbers offline? • What would we do differently tomorrow?

Key decisions and good practices to look for

- Call the bank's fraud line immediately to request a recall
- File a complaint with the FBI at ic3.gov as soon as possible
- Reset credentials, revoke sessions, remove malicious inbox rules, and enforce multi-factor authentication (MFA)
- Review mailbox access logs to determine data exposure
- Adopt call-back verification on a known number for all bank changes

Hotwash (last 15 minutes): What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.
Document it: the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.