FRAUD + CYBERSECURITY

Performing a proper callback

The importance of a validating callback cannot be stressed enough. This is the only true way to protect against BEC. However, there are multiple ways in which callbacks can go wrong, especially without formal procedures for performing callbacks.

As a ground rule, never use a phone number provided in an email. Your business should also have a set of checks that ensure a callback was performed. To help you create and enforce callback controls, here's more information on what to do and what not to do.

1 Don't rely on inbound phone calls

Always conduct an outbound call to the party to confirm they are legitimate.

Never ask that a vendor call you to validate payment instructions. **Never** use an inbound call to update contact information.

Why? Relying on inbound calls is an invitation for criminals to call you. If a fraudster has taken over a vendor's email, they'd know when you request that partner to call you. An outbound call from your staff to the party removes the risk that an employee falls prey to an enterprising criminal on the other end of the line.

2 Don't trust the number provided

Always use a known or trusted number for a system of record, and continually update any internal database for improved reference ability.

Never use a phone number provided to you in an email thread, invoice or attached documentation.

Why? Fraudsters will be all too happy to validate the transaction if you call them directly. Train staff to use this system of record repeatedly, as just one deviation from the controls opens the door to fraud.

3 Do speak with requestor

Always speak to the party who is personally accountable for the change in instructions.

Never settle for speaking with just any employee of the vendor that's initiated a payment or change.

Why? Fraudsters with email control will exploit messages between parties. Let's say your staff calls an accounting employee at the vendor, who then emails their own CFO for validation. What your staff and the vendor don't know is that cybercriminals have hacked the CFO's email and control it. This would allow fraudsters to circumvent your controls and direct the accounting employee under the presumed guise of the executive.

4 Don't assume internal controls have been followed

Always confirm controls were executed as intended and none of the above mistakes were made.

Never presume that a callback was performed.

Why? Human error happens; minimize its risk by actively ensuring procedures have been followed exactly as they were laid out.