REAL WORLD CASE STUDIES | COMPANION CHECKLIST

BEC Payment Fraud Governance Checklist

Wise Bites LLC | wisebitesllc.com

Five verification and control questions drawn from the case study on the Surfside Beach, South Carolina business email compromise. Answer each honestly before assuming your organization is already covered.

Verification Protocol

☐ We require a callback to a phone number already on file, never one supplied in the email or form requesting a change, before altering any vendor's payment method or banking details.

☐ Our policy states clearly what happens when that callback goes unanswered: a hold on the payment, not permission to proceed.

☐ Verification is documented as confirmed, a completed two-way conversation, not merely attempted, a message left or an email sent.

Segregation of Duties

☐ No single employee can both authorize a payment change and execute the transfer.

☐ A second reviewer signs off on any wire or ACH change above a defined dollar threshold.

Incident Response and Reporting

☐ Our incident response plan specifies a 72-hour reporting window to law enforcement and our insurer once fraud is suspected.

☐ That plan has been tested or tabletop-exercised within the last 12 months.

☐ Staff know exactly who to notify if a payment request feels even slightly unusual, without fear of slowing down a legitimate one.

Insurance and Recovery

☐ Our cyber insurance policy has been reviewed specifically for social engineering and BEC coverage, not just data breach coverage.

☐ We know our bank's fraud reporting line and wire recall process before we need them.

Bottom Line

Two or more unchecked items is not a technology gap. It is a governance gap, and one that is fixable in weeks, not months.