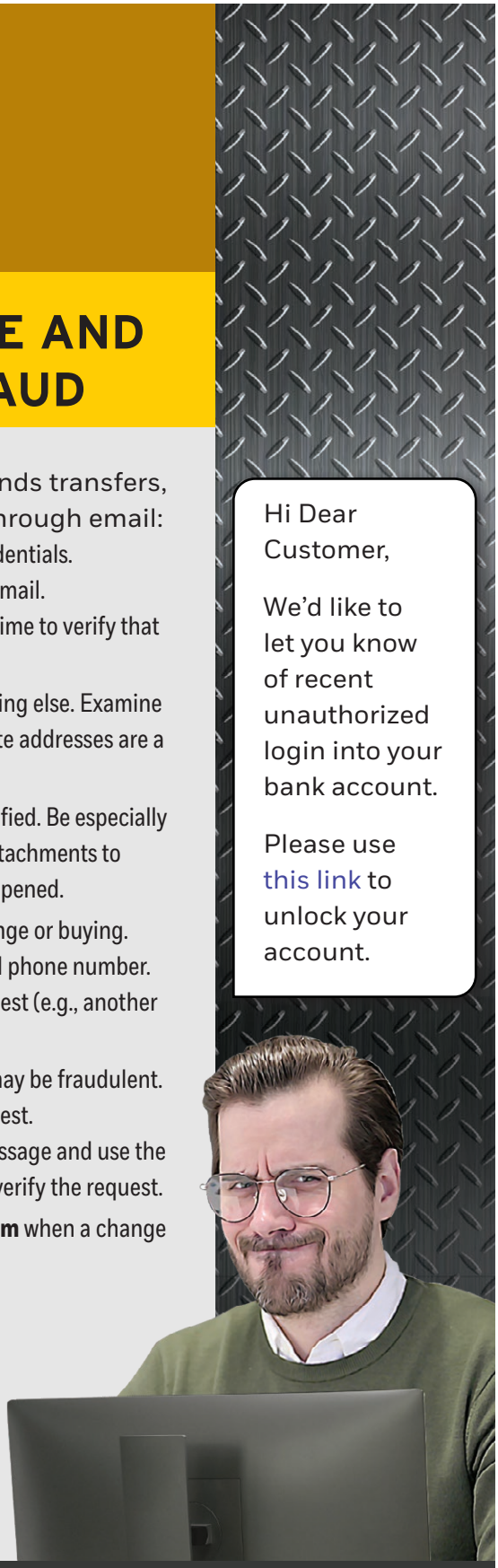
Loss Prevention
QUICK REVIEW
DATA SECURITY

# BUSINESS EMAIL COMPROMISE AND MISDIRECTED PAYMENT FRAUD

Follow these best practices to spot fraudulent requests for funds transfers, access to critical account credentials or to make purchases through email:

- **Be suspicious of all unsolicited requests** to update or verify account credentials.
  - Typically, legitimate partners do not make these requests through email.
  - Be especially wary if the sender is pressing you to act quickly. Take time to verify that the request is legitimate.
- **Look for signs that a message is a phishing attempt** before doing anything else. Examine spelling, the email address and link URLs. Slight differences from legitimate addresses are a hallmark of a scam.
- **Do not open attachments from senders you do not know** or have not verified. Be especially wary of attachments that have been forwarded to you. Hackers often use attachments to deploy malware, including ransomware, onto systems as soon as the file is opened.
- **Verify payment changes or purchase requests** before authorizing a change or buying.
  - Call the party making the request using a known, previously verified phone number.
  - If reasonable, you could personally visit the person making the request (e.g., another employee) to verify it.
- **Do not verify using email**, especially do not reply to the email you think may be fraudulent. You would just be asking the criminal to validate his or her fraudulent request.
  - When no other contact is available other than email, start a new message and use the known, previously verified email address for the partner contact to verify the request.
- Require the **payee** to **complete and sign a new direct deposit or ACH form** when a change is requested. Follow the verification techniques above.
- **Be suspicious of messages from Green Dot Bank.** This online bank is frequently used in misdirected payment fraud scams.
- **Do not make changes if you are not authorized to do so** for direct deposits, ACHs, fund transfers, account details and the like. We limit the number of people authorized to do this.
- **Investigate unusual requests**, ask questions and verify the authenticity of the request.




If you are unsure of any request that comes to you, please take it to your supervisor before doing anything else.

Click Wisely