BUSINESS EMAIL COMPROMISE

Help protect your company and accounts from the most popular method of fraud.

Fraudsters use various email tactics to con their victims. These methods include:

- Impersonating vendors in emails, directing payments (based on authentic invoices) to fraudsters' accounts
- Pretending to be other third parties in emails, requesting changes in bank account(s), payment instructions, etc.
- Emails requesting change in payroll bank information from an employee
- Faxes requesting revisions in bank instructions

82 percent of financial professionals experienced attempted and/or actual payments fraud in 2018*

The percentage of organizations falling prey to BEC scams has increased from 64 percent in 2014 to 80 percent in 2018:

- Wire transfers were 43% of BEC payment methods
- ACH credits were 33% of BEC payment methods
- ACH debits were 21% of BEC payment methods

BEST PRACTICES TO HELP MITIGATE BUSINESS EMAIL COMPROMISE

- **Verify any account changes** for an employee (payroll) or vendor (invoice) by reaching out directly to that employee or vendor using existing, previously known contact information
- **Confirm any payment instructions** received via email or fax with the requestor by reaching out via another communication method, ie: separate email or phone call
- **Adopt a two-factor authentication** or other added security for access to payments initiation
- **Avoid opening email attachments** or clicking on internet links in suspicious emails
- **Be suspicious** of requests that stress urgency, secrecy or the need to act without further confirmation

IF YOU SUSPECT FRAUD CONTACT YOUR RELATIONSHIP MANAGER

SEE SOMETHING. SUSPECT SOMETHING. SAY SOMETHING.

*Source: 2019 AFP Payments Fraud and Control Survey