BANC OF CALIFORNIA | TOGETHER WE WIN®

PROTECT YOUR BUSINESS AGAINST PAYMENT FRAUD

Recognize it. Resist it. Report it.

Payment fraud is a growing problem that every organization needs to guard against.

Payment fraud can happen to your business at any time; you pay what you believe is a legitimate invoice from a legitimate vendor or contractor, but the payment actually goes to an impostor who may be anywhere in the world and virtually impossible to find. Beyond the financial loss, it can also result in exposure of confidential company information and can spread malware and spyware to gain access to confidential personnel and customer information.

If Payment Fraud happened to you, you wouldn't be alone. In a recent Association of Financial Professionals® (AFP) survey, 82 percent of financial professionals reported that their organizations were targeted in 2018.*

Business Email Compromise (BEC) is an increasingly common scam.

BEC, also known as Email Account Compromise (EAC), targets business officers who execute payments. The targeted individual receives an email from what appears to be a known vendor, contractor or other third party – often a senior executive. The email requests an urgent transfer, invoice payment, and/or a change in bank account or payment instructions (e.g., new routing and account information for ACH or wire payments, a change of payment method from check to ACH, or changes in banking information for payroll). Some fraudsters impersonate HR departments, directing employees to sign in using what appear to be official links.

Fraudsters have become stunningly skilled at impersonation.

Fraudsters are more sophisticated than ever and can stalk their victims with great efficiency. Using phishing emails and social engineering techniques via social media, they learn all they can about their targets' patterns, habits and mind-set. They poach contacts and other information. They learn what payment methods their potential victims use, so their requests can appear routine.

Another tactic is to create a fake account and let it sit for months so that when it appears, no-one is alerted by a new vendor or contractor.

They can also hack into the officer's account and use it at will, with no way for anyone to tell. They often use social media or "out of office" messages to time the attack for when the officer is away.

Sources of Attempted and/or Actual Payments Fraud in 2018*

(percent of organizations that experienced attempted and/or actual payments fraud)

64% **Outside Individual**
(e.g. check forged, stolen card)

58% **Business Email Compromise**
(BEC Fraud)

22% **Third-Party or Outsourcer**
(e.g. vendor, professional services provider, business trading partner)

21% **Account Takeover**
(e.g. hacked system, malicious code – spyware or malware from social network)

What can you do to protect against payment fraud? Read on to see 10 measures you can take.

* 2021 AFP® Payments Fraud and Control Survey | www.AFPonline.org

10 WAYS TO GUARD AGAINST BUSINESS PAYMENT FRAUD

1 Isolate and safeguard your payment system

- Use a dedicated computer to process payments.
- Choose hardware, software and service providers that meet security validation requirements.
- Always use anti-virus software and keep it updated, to keep your IT systems from viruses and malware.
- Use a secure system for remote access or eliminate remote access if you don't need it.
- Never provide nonpublic business information on social media.

2 Protect your email account and devices

- Never, ever provide your login credentials to anyone.
- Do not use the "reply" option when authenticating emails for payment requests. Instead, use the "forward" option and enter the correct email address by typing it or selecting it from your address book.
- Do not use free web-based email accounts. Business emails should always use company domains.

3 Verify all payment and change requests

- Require that all payments and/or changes (e.g., account or routing transit numbers, payment type, amount, financial institution, mailing address, etc.) be separately verified and approved by different people.
- Use a different communication channel than the one the request came in on. For large payments, use multiple channels.
- Never use the contact information from the request; always use the contact information you have on file.
- Make vendor payment forms available only to appropriate personnel, using secure means.
- Require that any changes to payment account information be made or confirmed by a system administrator, using methods like verification codes for existing contacts.
- If a financial institution questions the legitimacy of a payment, respond quickly.

4 Limit access, implement dual custody and segregate functions

- Limit access to payment systems to employees who need it.
- Break down the payment process into separate steps and divide those steps between two people. The same person should not be able to both create and approve a payment.
- Segregate accounting duties, so there is dual custody.

5 Teach your employees to recognize and resist potential fraud and provide tools to report it

- Educate and train employees to question and independently authenticate changes in payment instructions. They should never fall prey to requests for secrecy or pressure to take action quickly.
- Urge them to be skeptical even when the outreach appears to legitimately be from the requesting organization.
- Make sure they are always aware of the tell-tale signs including typos, grammatical errors, missing words, payment amounts that differ from the invoice, use of a public email domain such as Gmail, subtle changes in the organization's name in the email address requests to pay individuals, or anything that does not exactly match the information you have on file.
- Make sure they know not to open attachments, click links or give any personal information, as fraudsters use these to install malicious malware.
- Refer them to government agency websites that provide information and advice about recognizing and responding to suspected fraud and links to report it. These include: **FBI FCC FTC.**

6 Implement background checks and rigorous monitoring protocols

- Review past payment history to detect any deviation from the typical pattern.
- Perform account reconciliations regularly.
- Review vendor address and banking information changes and request supporting documentation to confirm any changes.
- Review personnel changes.

10 WAYS TO GUARD AGAINST BUSINESS PAYMENT FRAUD

7 Teach your employees to be wary of fake check scams

- Teach employees to be alert to check scams in which a scammer sends a (bad) check for more than has been billed to the targeted vendor or contractor and asks you to wire the overage to a third party. This scam often includes a reason for the overpayment and an immediate need for the reimbursement. When the bank discovers the bad check, you'll be responsible for any payments made against it.
- Guard your checks and check stock carefully. Scammers may steal them and defraud you by "check washing" – deleting your information and changing the payee's name and, possibly, the amount.

8 Use positive pay to protect against check fraud

- **Positive Pay** continues to be the method most often used by organizations to guard against check fraud.
- It helps identify fraudulent checks by matching check issue information against checks presented for clearing, and sends electronic notification alerts of any discrepancies, so you can decide whether to pay or return it.
- **Payee Positive** Pay provides a second security layer to our standard Positive Pay with Payee name matching.
- If a discrepancy appears, you will receive electronic notification alerts which require your decision to pay or return the item.

9 Use ACH Positive Pay and ACH Block to combat wire transfer fraud

- **Business Online Banking** provides advanced anti-fraud features and a wide range of self-service banking capabilities.
- **ACH Positive Pay** enables you to establish and control acceptable sender parameter profiles. You can view any ACH debit outside of your sender parameter profiles and either pay or return it. ACH anti-fraud services include features to help avoid inadvertently rejecting authorized ACH payments.
- **ACH Block** provides the ability to block all ACH debits, or those of specific originators, from being posted to your account. All blocked transactions will be automatically returned to the originator.

10 Help your employees guard against payroll impersonation

- Train your employees to watch for phishing attacks and suspicious malware links and to carefully examine the sender's address of any emails they receive.
- They should know not to reply to any suspicious email or enter login credentials when clicking on a link or opening attachments.
- Employer self-service platforms should authenticate requests to change payment information using previously known contact information. One method is to require "Out of Band Authentication" – a second password that is sent in an SMS text message or to an existing email address, or to use a hard token code. They should also reauthenticate users accessing the system from unrecognized devices, using previously known contact information.
- Set up administrator alerts on self-service platforms for unusual activity such as a change in banking information or when multiple changes that use the same new routing number or identical account numbers. Also, consider validating any new Direct Deposit information by sending ACH prenotification transactions.

HOW TO REPORT PAYMENT FRAUD:

If you believe you are the victim of payment fraud, contact the **FBI Internet Crime Complaint Center (IC3).**

If you suspect a payment fraud attempt but have not lost money, contact **FTC Report Fraud.**

If you believe your account information has been disclosed, contact **Banc of California.**

BANC OF CALIFORNIA | TOGETHER WE WIN®