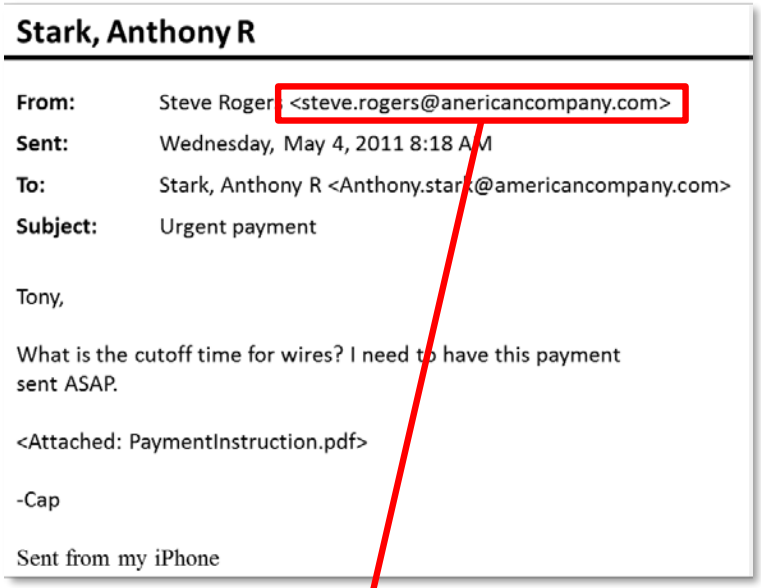
Insights for governments on cybersecurity and fraud prevention

In an ever-growing digital environment

August 2020

What is Business Email Compromise (BEC)

A scam where the fraudster hacks, spoofs, or masquerades a business email account in order to access the company and perform fraudulent transactions.



Stark, Anthony R

From: Steve Rogers <steve.rogers@anericancompany.com>
Sent: Wednesday, May 4, 2011 8:18 AM
To: Stark, Anthony R <Anthony.stark@americancompany.com>
Subject: Urgent payment

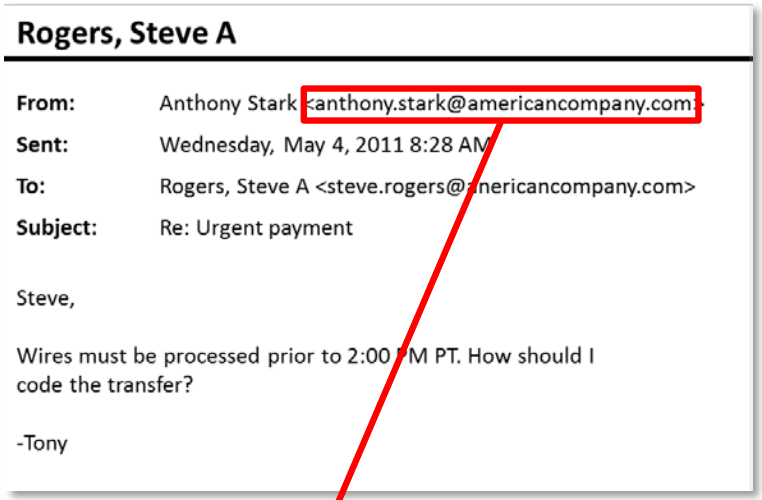
Tony,

What is the cutoff time for wires? I need to have this payment sent ASAP.

<Attached: PaymentInstruction.pdf>

-Cap

Sent from my iPhone



Rogers, Steve A

From: Anthony Stark <anthony.stark@americancompany.com>
Sent: Wednesday, May 4, 2011 8:28 AM
To: Rogers, Steve A <steve.rogers@americancompany.com>
Subject: Re: Urgent payment

Steve,

Wires must be processed prior to 2:00 PM PT. How should I code the transfer?

-Tony

<steve.rogers@anericancompany.com>

<anthony.stark@americancompany.com>

See end disclosures.

Business email compromise (BEC) is on the rise

$12B	total and potential losses globally since 2013
24K	complaints reported to the FBI in 2019
$1.7B	adjusted losses during 2019
1/3rd	of cases highlight a payment through wire transfer
11%	of all email fraud attacks use ‘fake email chain’ messages

Source: InfoSec Magazine - https://www.infosecurity-magazine.com/news/bec-attacks-jumped-17-last-year/
See end disclosures.

Identifying types of BEC

The “Executive Masquerade”

Spoof	Masquerade	Funds Transferred
• The email accounts of high-level business executives (Chief Financial Officer, Chief Technology Officer, etc.) are compromised. • The account may be spoofed or hacked.	• A request for a wire transfer from the spoofed account is made to a second employee responsible for processing requests. • In some instances, the request is sent directly to the financial institution with instructions to urgently send funds to bank “X” for reason “Y.”	• The victimized employee processes the fraudulent request. • The fraudster receives the funds.

Sources: 2017 FBI PSA: https://www.ic3.gov/media/2017/170504.aspx;
U.S. Bank Financial IQ – Minimize Risk: https://financialiq.usbank.com/index/improve-your-operations/minimize-risk.html
See end disclosures.

The “Supplier Swindle”

Spoof	Masquerade	Funds Transferred
• A business with a relationship with a supplier is requested to wire funds for an invoice payment to an alternate, fraudulent account. • The request may be made via telephone, facsimile, or e-mail. • The communications are spoofed in similar fashion to the “Executive Masquerade.”	• A request for a wire transfer from the spoofed communication is made to an employee at the business responsible for processing requests.	• The victimized employee processes the fraudulent request. • The fraudster receives the funds.

Sources: 2017 FBI PSA: https://www.ic3.gov/media/2017/170504.aspx;
U.S. Bank Financial IQ – Minimize Risk: https://financialiq.usbank.com/index/improve-your-operations/minimize-risk.html
See end disclosures.

Demo—Email Spoofing

1 Spoof from: Timber Insurance
Reply To: @yahoo.com

Funds from **Victim**

2

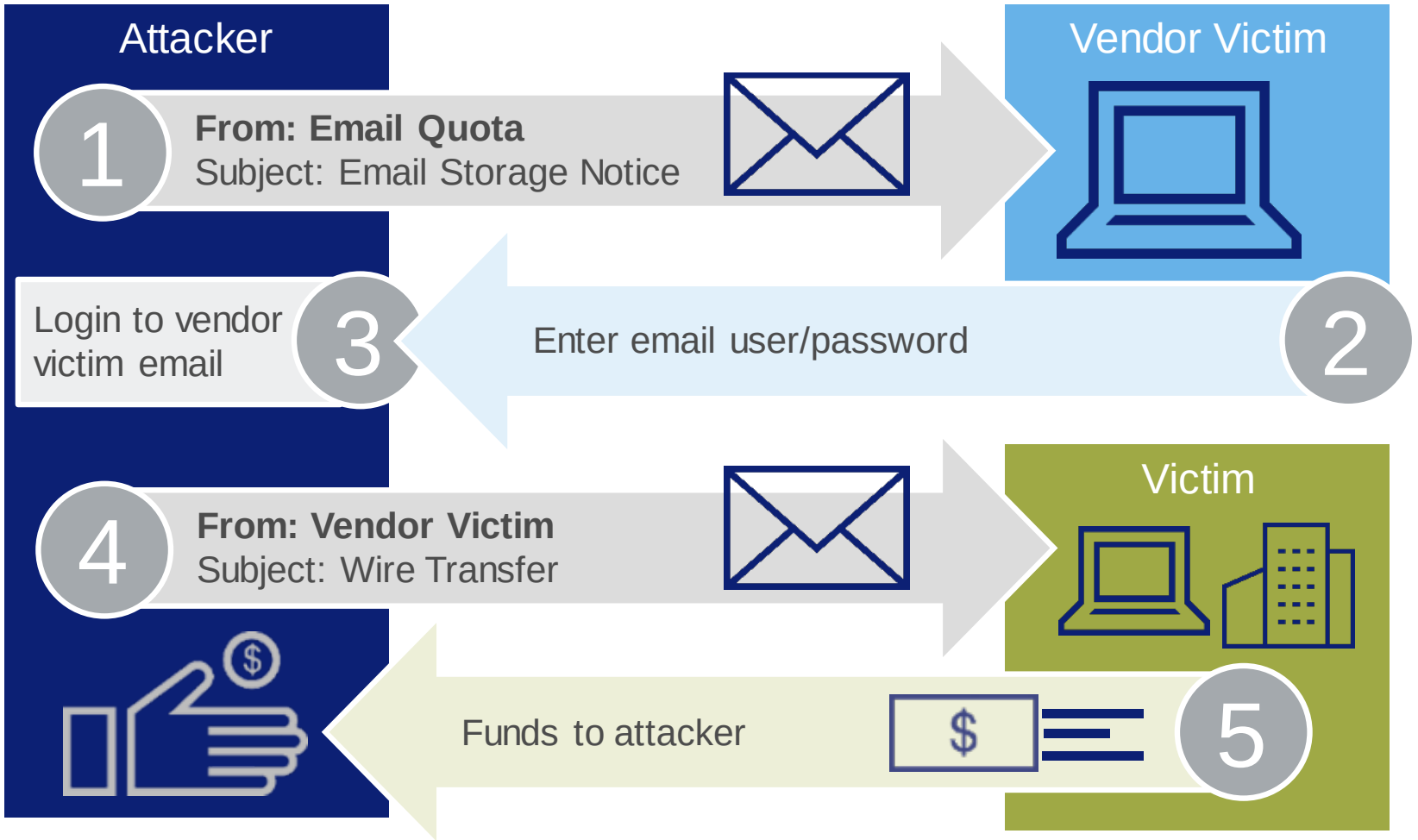
See end disclosures.

The “Hack Job”

Hack	Masquerade	Funds Transferred
• An employee of a business has his or her personal email hacked. • This personal email may be used for both personal and business communications.	• Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee’s personal email to multiple vendors identified from this employee’s contact list.	• The victimized employee processes the fraudulent request. • The fraudster receives the payment. • The business may not become aware of the fraudulent requests until that business is contacted by a vendor to follow up on the status of an invoice payment.

Sources: 2017 FBI PSA: https://www.ic3.gov/media/2017/170504.aspx
See end disclosures.

Demo—Email Credential Theft



See end disclosures.

The “Lawyer Up”

Spoof	Masquerade	Funds Transferred
• Fraudsters typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. • Contact may be made via either phone or e-mail.	• Victims pressured by fraudster to act quickly or secretly in handling the transfer of funds. • Typically occurs at the end of the business day or work week. • Timed to coincide with the close of business of international financial institutions.	• The victimized employee processes the fraudulent request. • The fraudster receives the payment.

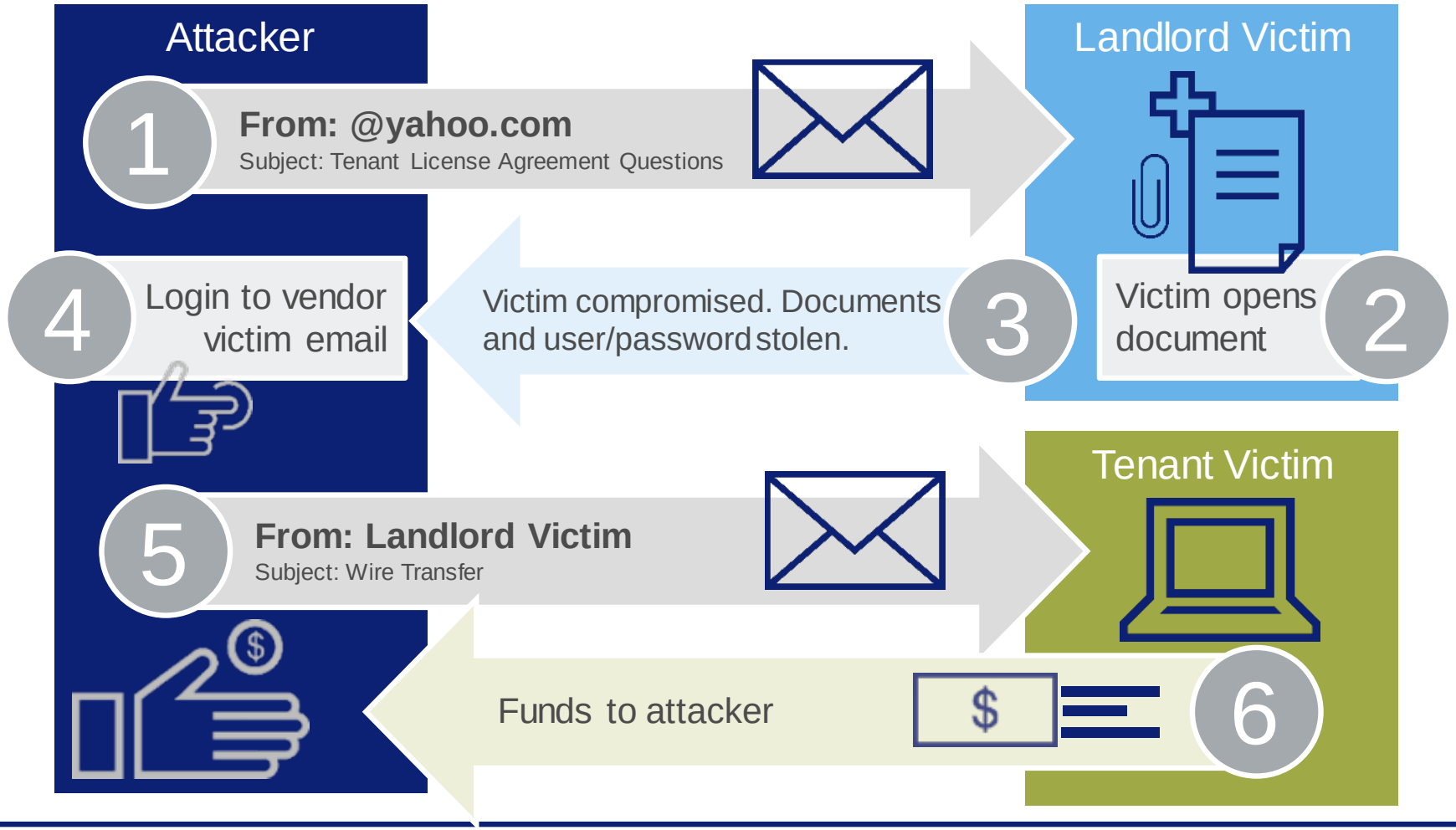
Sources: 2017 FBI PSA: https://www.ic3.gov/media/2017/170504.aspx
See end disclosures.

The “Data Dump”

Spoof	Masquerade	Data Transferred
• The email accounts of high-level business executives (Chief Financial Officer, Chief Technology Officer, etc.) are compromised. • The account may be spoofed or hacked.	• Business personnel responsible for W-2s or maintaining PII, like human resources, bookkeeping, or auditing, are targeted. • The fraudster requests W-2 and/or PII information. • Incidents can be isolated and some occur prior to a fraudulent wire transfer request.	• The victimized employee processes the fraudulent request. • The fraudster receives the data. • Victims have fallen for this scenario even when they successfully identify and avoid the traditional BEC scam.

Sources: 2017 FBI PSA: https://www.ic3.gov/media/2017/170504.aspx; U.S. Bank Financial IQ
See end disclosures.

Demo—Hacking



See end disclosures.

Prevention strategies and response

Staying safe online

Your cyber posture at home impacts your cyber posture at work.

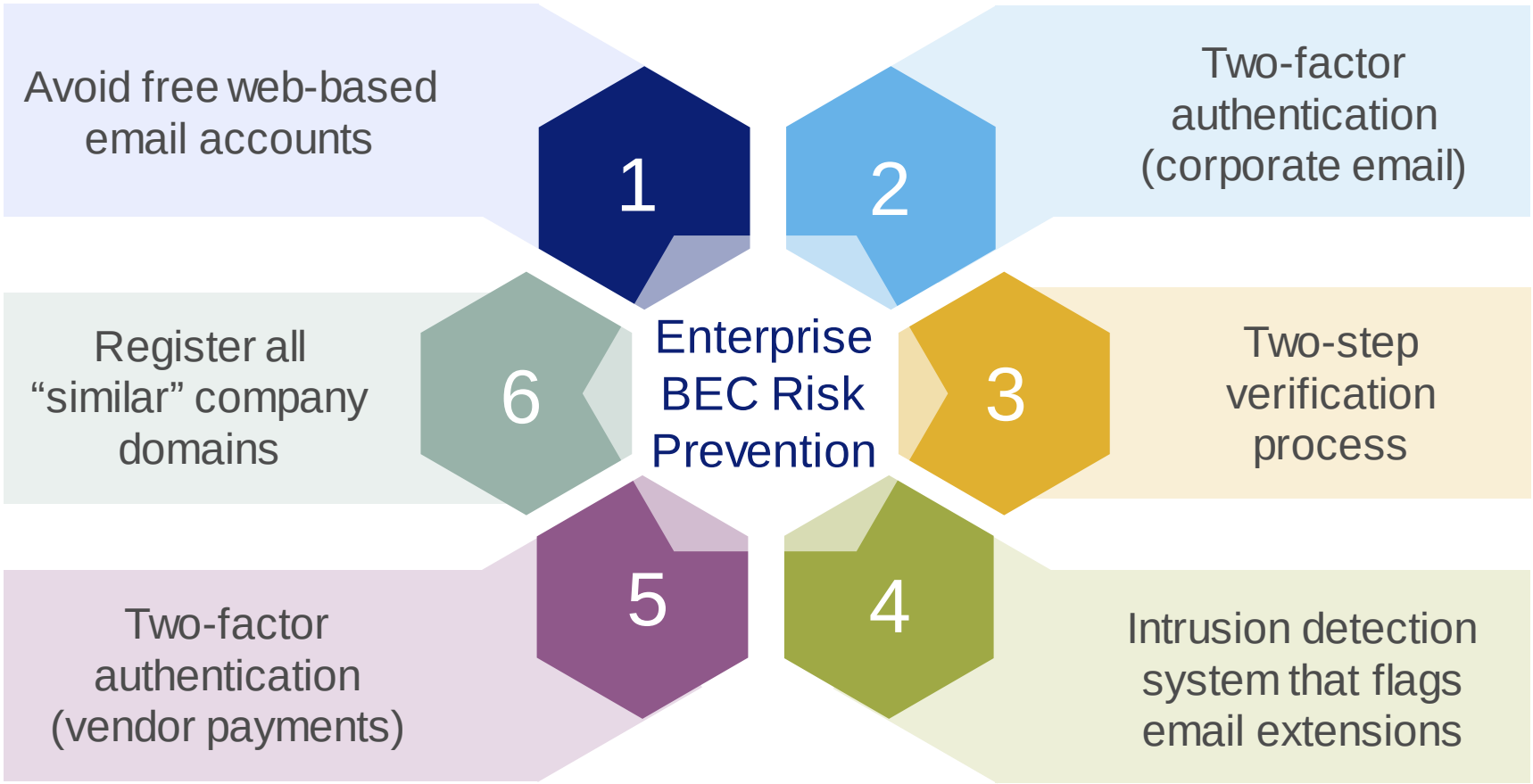
Beware of unsolicited offers.

- Reconnaissance can be easily conducted on **LinkedIn, Facebook, and Instagram**.
- **On social media, phishers can learn:**
  - **1)** your employer
  - **2)** your position
  - **3)** your current location (geo-location)
  - **4)** products and subjects that you "like" or find interesting
  - **5)** your connections like friends, family and even co-workers

  Your interests inform phishers on how to target you.
- A phisher can guess your work email address **(e.g., jane.doe@governemntagency.gov).**

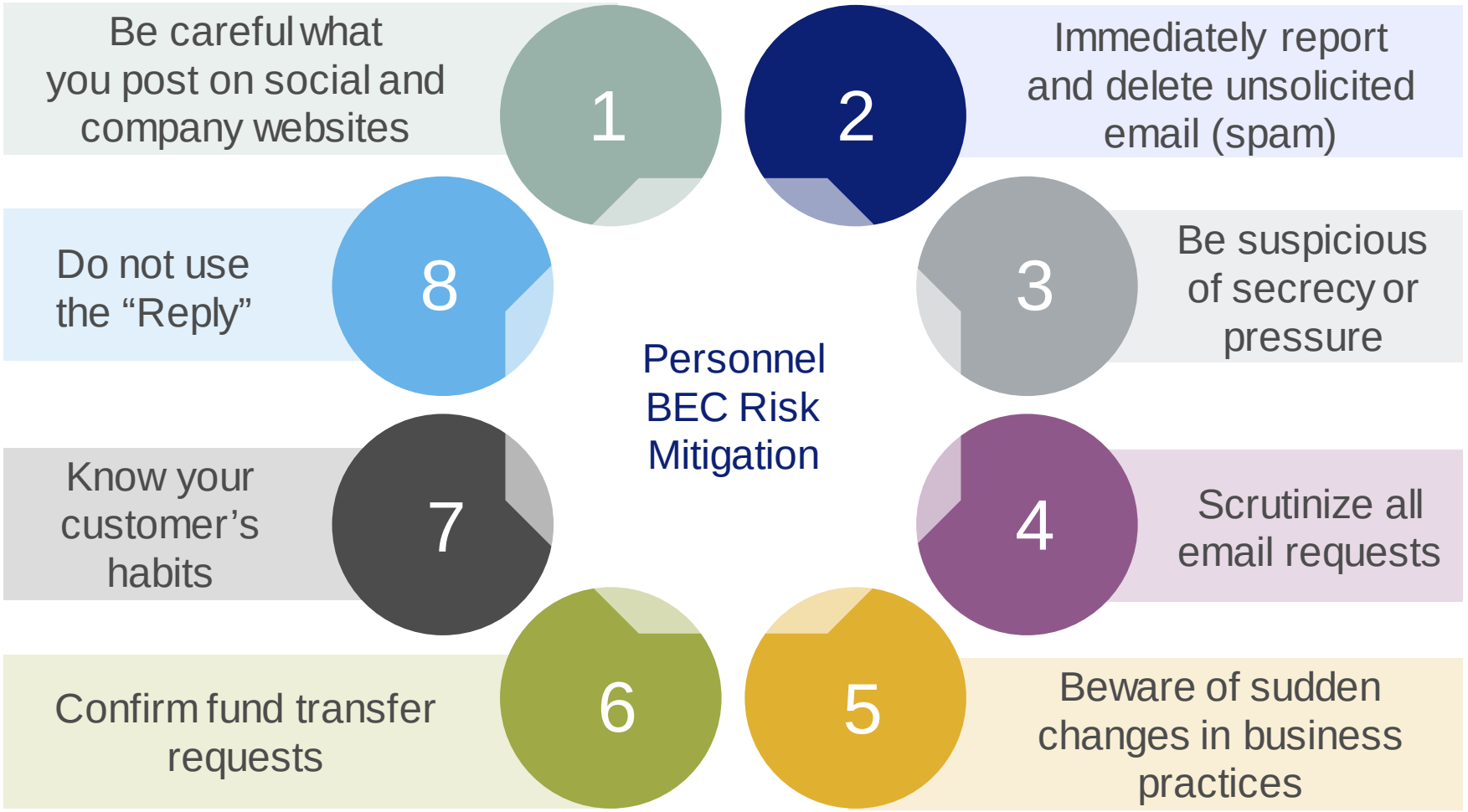
See end disclosures.

Prevent risk with enterprise strategies



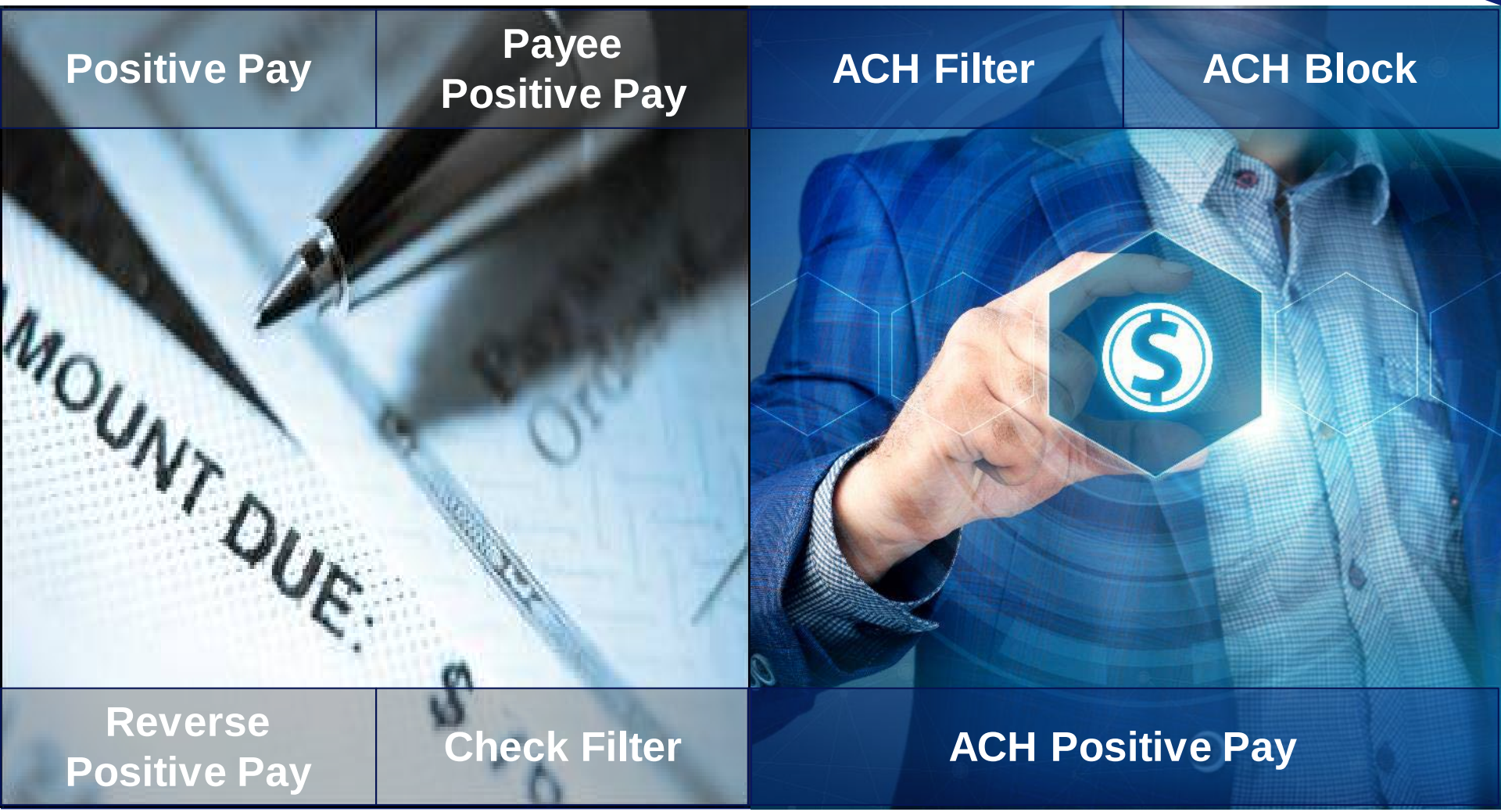
Sources: 2017 FBI PSA: https://www.ic3.gov/media/2017/170504.aspx;
U.S. Bank Financial IQ – Minimize Risk: https://financialiq.usbank.com/index/improve-your-operations/minimize-risk.html
See end disclosures.

Mitigate risk with personnel policies



Sources: 2017 FBI PSA: https://www.ic3.gov/media/2017/170504.aspx;
U.S. Bank Financial IQ – Minimize Risk: https://financialiq.usbank.com/index/improve-your-operations/minimize-risk.html
See end disclosures.

Inquire about protective banking services



See end disclosures.

Act immediately—your fraud response

Contact
Commercial Customer Service (CCS)
to open a fraud case

Contact your local FBI Office
and file a complaint

Save all messages
and evidence

Sources: 2017 FBI PSA: https://www.ic3.gov/media/2017/170504.aspx
See end disclosures.

Q&A discussion

See end disclosures.

Disclaimers

These websites, and the services provided, are under the exclusive control of the respective third-party provider. These links are provided as a courtesy and do not imply, suggest, or constitute any sponsorship, endorsement, or approval of any third party or any affiliation with any such third party. Further, we make no warranties or representations whatsoever with regard to any third party website, merchandise, or service, and we are not responsible or liable to you for any damages, losses, or injuries of any kind arising out of your use of any third party website.

This information has been obtained from sources believed to be reliable, but we cannot guarantee its accuracy or completeness.