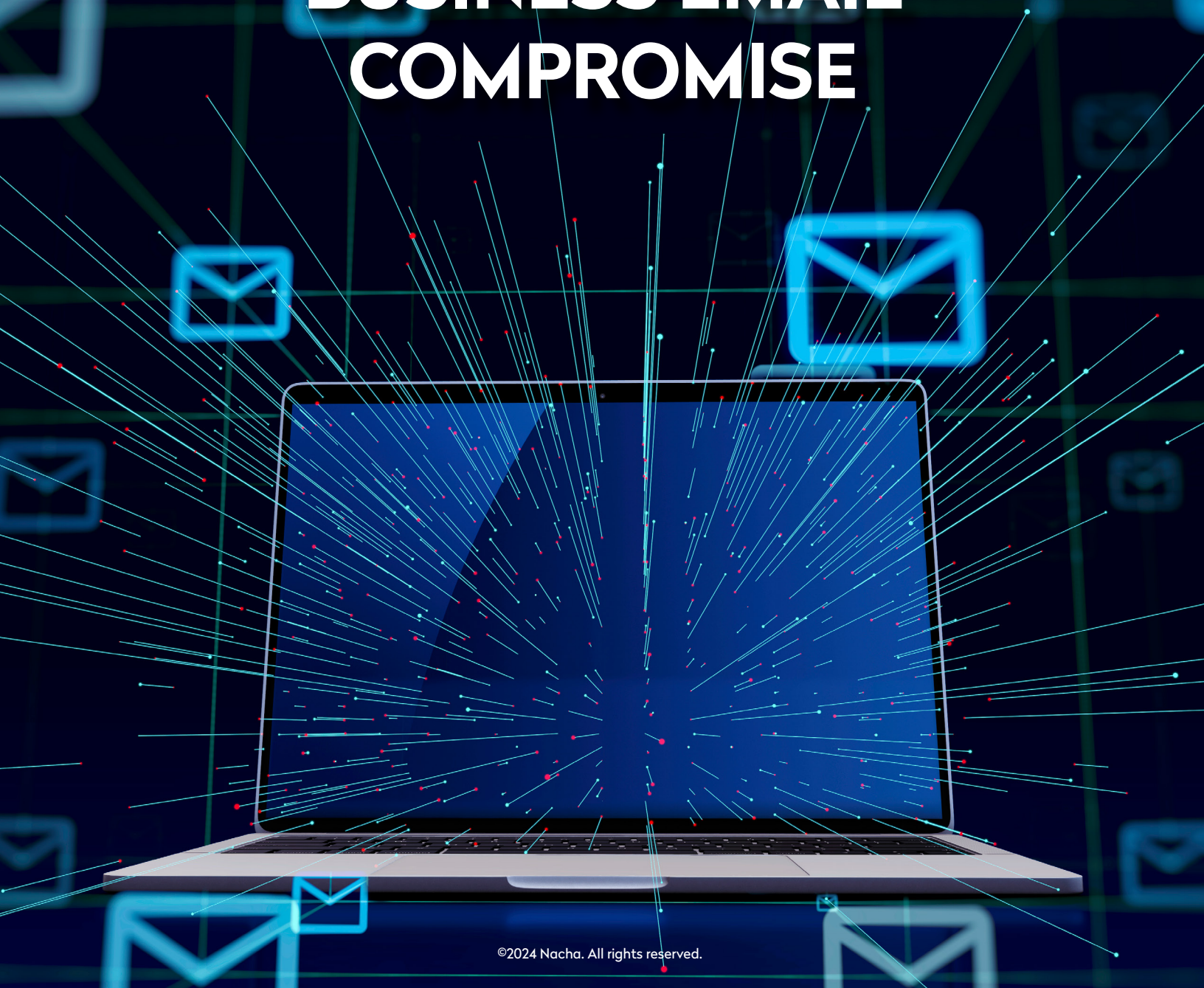
Payments Innovation Alliance®

RESPONSE ACTION PLAN BUSINESS EMAIL COMPROMISE



RESPONSE ACTION PLAN
BUSINESS EMAIL COMPROMISE

Business email compromise (BEC)—also known as email account compromise (EAC)—is one of the most financially damaging online crimes. It exploits the fact that most businesses rely on email to conduct personal and professional business. The FBI's 2023 Internet Crime Complaint Center (IC3) Report shows $2.9 billion in losses due to BEC in 2023.

In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request. For example, a known company vendor will appear to send an invoice with an updated payment address or payment account information. These scams have resulted in substantial financial and reputational harm to corporate victims.

Information that is shared publicly about contracts and business relationships make organizations vulnerable. Governmental, public finance and higher education entities that are required to post relationships as a matter of public record are easy targets. Company websites sharing management relationships between employees can be used to impersonate authorized requests.

This Response Action Plan ("Plan") is intended to guide companies that are victims of business email compromise and provide steps your company can take to mitigate the potential for being a victim.

What to do if your company is a victim?

REPORT & RECOVER

Act Fast to Recover Money

- If **you** sent money to a fraudulent account, **immediately** contact your financial institution and request that they contact the financial institution where the transfer was sent and ask them to reverse the transaction and freeze the fraudulent account.
- If **your customer** or trading partner sent money to a fraudulent account instead of paying you, ask them to contact their financial institution **immediately** to recover fraudulently transferred funds and freeze the fraudulent account.

Contact Law Enforcement

- **Contact your local FBI field office** to report the crime and **file a complaint** with the FBI's Internet Crime Complaint Center (IC3).
- Your company may also report the crime to Homeland Security Investigations' Cyber Crimes Center by completing the Online ICE Tip Form or calling 1-866-DHS-2-ICE.
- Contact local law enforcement and **file a police report**.
- Request that your law enforcement contact **work with IC3's Recovery Asset Team** (RAT) to liaise with financial institutions to recover your stolen money. Contact RAT through your local FBI field office.
- **Notify applicable regulators and licensing authorities** (including state and federal agencies) as required. For examples of regulators and licensing authorities who may need to be notified in the event of a security incident or breach, please see the Payments Innovation Alliance's Security Incident Response Procedure Guide.

RESPONSE ACTION PLAN
BUSINESS EMAIL COMPROMISE

Check and Keep Fraudsters Out

- **Scan and scrub all communications systems** for viruses, malware and other intrusions and security gaps, including email forwarding rules. Keep records of any viruses, malware or other intrusions that have been removed.
- Require employees to **change passwords immediately** and use strong passwords.

Document and Recover

- **Preserve all communications and records** related to the scam, including email communications and the IP address records used by the fraudster to access the company's systems. This information will be helpful to law enforcement.
- **Review insurance coverage** to determine whether coverage is available in the event of financial loss and provide notice to the insurance carrier.

PREVENT BEC SCAMS

- Implement and enforce **two-factor (or multi-factor) authentication** on any account that allows it.
- Implement a **two-step process** with customers, vendors and business partners whereby any changes to account information or other payment instructions are confirmed outside of the communication method or channel requesting the change to payment instructions.
- Establish internal **multi-layer review procedures** for approving transactions above certain thresholds. These procedures should include dual controls for approval of certain transactions and delegations of authority when one or both of the dual-control approvers are unavailable.
- Take advantage of SMS activity alerts that can be established with your financial institution(s) and **review all bank and payment card statements** for unusual activity daily.
- **Raise awareness** of how easily scams can occur and provide a written procedure to address situations and training for all employees on best practices to stop scams.
    - Use caution when sharing information online or on social media. By openly sharing things like pet names, schools you attended, links to family members and your birthday, you can give a scammer the information they need to guess your password or answer your security questions.
    - Refrain from posting on social media that you are on vacation. (Save those pictures for when you get back!)
    - Don't click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company's phone number either from an internal directory or a public directory on your own (don't use the one a potential scammer provides).
    - When communicating sensitive information, first ensure the person you are communicating with is the person you intended to talk to. Then confirm the other person's identity using a passcode, passphrase or other means of authentication.

RESPONSE ACTION PLAN
BUSINESS EMAIL COMPROMISE

- Carefully **examine the email address, URL, and spelling used in any correspondence**. Scammers use slight differences to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.
- Fraudsters can "spoof" phone numbers to trick you, so the caller ID may display a valid name or something that looks like your vendor's name. If you receive a phone call requesting a change in account number or payment procedures, call the requester back on a known phone number.
- If unsure if a request may be fraudulent, ask your internal resources to help.
- Implement and train all employees on **best practices** for email and online activity security.

- Be especially **wary if the requestor is pressing you to act quickly**. If employees have questions or concerns, provide internal resources, such as legal and compliance contacts.

Cybersecurity & Payments AI Project Team

This Plan was developed by the Cybersecurity & Payments AI Project Team of Nacha's Payments Innovation Alliance, with special recognition to Matt Luzadder with Kelley Drye & Warren LLP.

The Payments Innovation Alliance is a membership program that shapes the future of the payments industry and develops thought leadership relevant to financial service institutions. The Alliance established the Cybersecurity & Payments AI Project Team to help organizations understand and respond to evolving threats related to potential cyberattacks. Visit Cybersecurity & Payments AI Project Team to see more resources developed by the team.

Payments Innovation Alliance®