Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

BUSINESS EMAIL COMPROMISE (BEC) – AI THREAT

SUMMARY

Industry reporting shows AI (artificial intelligence) is increasingly enhancing the quality of fraudulent emails, making real incidents harder to detect and highly lucrative for attackers. AI is supercharging phishing and BEC (business email compromise) techniques, including AI-crafted impersonation emails that tailor tone and context to specific recipients—making fraudulent transfer requests and change of account information more believable. Financial Institutions are seeing more convincing, targeted scams that mimic internal requests, often enabled by generative AI.

OVERVIEW OF THE RISK

BEC fraud has traditionally relied on compromised email accounts and social engineering. However, fraudsters are now leveraging AI tools to significantly enhance the sophistication, scale, and success of these attacks.

AI-enabled BEC schemes may include:

- **AI-generated emails** that closely mimic writing style, tone, and vocabulary of executives, vendors, or accountholders
- **Deepfake voice or video impersonation** used to pressure staff into urgent wire, ACH, or account changes
- **Automated reconnaissance** to analyze publicly available information (websites, social media, filings) and tailor highly targeted requests
- **Real-time language translation and refinement,** enabling convincing fraud attempts across regions and business relationships

These tactics increase the likelihood that fraudulent payment requests or account changes may bypass traditional red flags.

RECOMMENDED MITIGATION MEASURES

Financial institutions should consider strengthening controls in the following areas:

Payment and Account Change Controls

- Enforce **out-of-band verification** (known phone numbers, call-backs) for all payment instructions, wire requests, and vendor/member account changes
- Prohibit reliance on email alone for authorization of high-risk transactions
- Establish dollar thresholds requiring dual control or supervisory approval

Employee Awareness and Training

- Update fraud training to include **AI-driven BEC scenarios,** including realistic examples
- Reinforce a "pause and verify" culture—urgency and secrecy are key fraud indicators
- Train staff to challenge requests that deviate from established procedures, even when they appear authentic

Email and Technology Controls

- Implement or review **email authentication standards** (SPF, DKIM, DMARC)
- Utilize advanced email security tools capable of detecting impersonation and anomalous behavior
- Restrict public exposure of employee roles, contact information, and approval authority where feasible

Education

- Educate business members on BEC and AI-driven fraud risks
- Encourage vendors and accountholders to use **secure communication channels** for payment changes
- Promote written agreements outlining verification requirements for payment instructions

Incident Response Preparedness

- Maintain clear procedures for responding to suspected BEC events
- Act quickly to notify financial partners, law enforcement, and insurers when fraud is suspected
- Periodically test response plans through tabletop exercises

AI-enhanced fraud is rapidly lowering the barrier for criminals and increasing the realism of impersonation attacks. Financial Institutions should assume these tactics will continue to evolve and proactively assess whether existing controls are sufficient to address this emerging risk.

We encourage financial institutions to review their policies, procedures, and training programs to ensure preparedness against AI-enabled BEC threats.

RISK MITIGATION RESOURCES

- Register for Experian's *"Future of Fraud Forecast"* Webinar on February, 5th
- Read: *"Rising Incidents of BEC and Wire Fraud"*

- Read: *“Seized Funds Phishing Attempt via JP Morgan Chase & Co Impersonation”*
- Learn about corporate fraud and deepfake AI attacks from Cybersecurity-Insiders.com
- Sign up for our Let’s Talk Fraud quarterly webinars
- View additional risk resources
- Visit our **NEW** Fraud Prevention Center!

Contact our risk specialists at risk_specialist@alliedsolutions.net

The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.

LinkedIn