Are Cyber Thieves Compromising E-Mail? .. YES!

Recently FinCEN issued Advisory (FIN-2016-A003) regarding e-mail compromise schemes that defraud Financial Institutions by deceiving them into conducting wire transfers that result in misappropriated customers funds. The cyber-criminals are "impersonating" victims, and submitting what seem to be legitimate wire transfers instructions for Financial Institutions to execute.

There are (2) main types of e-mail fraud:

1. **BEC**: Business E-mail Compromise targeting a Financial Institutions' corporate/commercial accounts.
2. **EAC**: E-mail Account Compromise targeting Financial Institutions' individual/personal accounts.

Preventing unauthorized wire transfers performed by Financial Institutions requires yet another layer of due diligence by Financial Institutions. FinCEN, together with the FBI and the US Secret Service, developed a list of Red Flags for Financial Institutions to consider for identifying and preventing E-mail fraud schemes. The "**Red Flags"** are for E-mailed wire transactions instructions that:

- Contain different language, timing, and amounts that vary from a customer's previously verified/authenticated e-mailed transaction instructions.
- Contain an email address that has been slightly altered (adding, changing or deleting characters).
- Directs payment to a known beneficiary, but the beneficiary's account information is different than what was previously used.
- Directs wire transfer to foreign bank accounts that have been documented in customer complaints as a destination for fraudulent transactions.
- Directs payment to a beneficiary with no customer payment history or business relationship and the payment amount is similar to what the customer has historically paid to beneficiaries.
- Contain "Urgent/Secret/Confidential" language in the request.
- Contain delivery of instructions written in a way that would not allow the Financial Institution time to confirm the authenticity of the request.
- Contain instructions from a newly authorized person on the account or from an authorized person that has not previously sent wire transfer instructions.
- Contain instructions on behalf of the customer that are based on e-mail communications originating from executives, attorneys or their designees, with an inability to verify the transactions with such executives, attorneys or designees.

Foodman CPAs and Advisors * 1201 Brickell Avenue * Suite 610 * Miami, Florida 33131
Tel 305 365 1111 * Fax 305 365 2244 * www.foodmanpa.com * **info@foodmanpa.com**

- Contain requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers and or vendors.

Email fraud schemes are costing a fortune. Financial Institutions need to identify, prevent and report E-Mail fraud schemes. There has to be collaboration amongst the internal AML, Business, Fraud and cybersecurity departments at Financial Institutions. Information Technology business practices should be secure and up-to-date with triggers in place to help detect fraud. Moreover, Financial Institutions need to collaborate with law enforcement in order to put an end to this type of cyber-attack.

Don't be a victim of your own making. Financial Institutions need to review and verify their customer's transactions in order to prevent possible losses.

Foodman CPAs and Advisors * 1201 Brickell Avenue * Suite 610 * Miami, Florida 33131
Tel 305 365 1111 * Fax 305 365 2244 * www.foodmanpa.com * **info@foodmanpa.com**