**Fides Insurance Group / Office of Risk Management**
**RISK ALERT**
**SOPHISTICATED WIRE TRANSFER SCAM**
**August 17, 2021, No. 2021-12**

**PLEASE READ!!!**

Direct deposit and wire scams are becoming increasingly common, and ever more sophisticated. Intelligent and capable seasoned professionals are falling victim. Please do not think you or anyone on your staff are immune – anyone can fall victim to these scams. Carefully review and verify every request regarding financial matters.

**RECENT SCAMS**

One of our institutions received a fraudulent letter via mail from a person claiming to be an employee of a health benefit provider. The person also followed up with an email to the Benefits Coordinator. The letter and email requested payment by electronic transfer instead of the usual method, which was via check. The email stated: "We prefer to receive payments via ACH or wire transfer going forward, this is due to our new billing system."

The letter and the email appeared to be from an actual employee of the health insurance provider; however, the email address was slightly different – one letter (an "s") was removed from the legitimate email and web address, making it easy to mistake the fraudulent email and address for the legitimate one. The scammers purchased the domain name without the "s" as part of their scam to defraud companies of money so that, upon a quick glance, the address appeared to be legitimate.

Several days after the institution initiated a payment via wire transfer per the email's instructions, the institution's bank contacted the institution's CFO, suspecting fraud. The CFO investigated the matter by contacting the health insurer, and it was determined that this was in fact a scam.

**Be on your guard and always take several steps before you respond to any request for payment or for a change in the method of payment. Scammers know that once you wire money to them, there is usually no way to get your money back.**

In another scam reported by a parish, the secretary received a request that appeared to be from a member of the parish staff asking that his bank account information for direct deposit be changed before the next pay day. The secretary forwarded the email to the business manager and cc'd the employee, at which point the employee informed them that the email did not come from him.

## To prevent these types of scams from happening to your parish or institution, please take the following steps:

- **A transfer of funds should never be performed solely on the basis of an email exchange. Obtain verbal confirmation** by calling your known contact directly.

- **Do not call the number listed in the email or on the letter you received.** If it's a fraudulent email or letter, the number will be fraudulent as well. Always call the legitimate number of your known contact.
- **Do not share bank account numbers or other banking information over email.** Banks will never ask for your account number, social security number, name, address or password in an email or text message. They will only ask you to provide this information to verify your identity when you call them directly.
- **Watch for Misspelled Words.** It's very common to find typos in a fraudulent email or text. If you find one in the message, it is most likely a scam.
- **If the tone of the email is urgent, this should be a signal for additional caution.** Never wire money to anyone who pressures you to pay immediately, or who says a wire transfer is the only way to pay.
- **Always look at the sender's email for clues of its legitimacy**. Examine the sender's email address closely, comparing it to previous emails or correspondence known to be legitimate. Scammers will use email addresses that look similar to a legitimate email, but you will usually find tell-tale signs that it's a fraud.
- **When in doubt, call the IT department or the Office of Risk Management**.

**REMEMBER: STOP – CALL – CONFIRM**

If you have any questions, please contact our office at jfm@rcab.org.