Office of Risk Management
RISK ALERT
No. 2021-05

RE: Email Wire Transfer Scam **April 1, 2021**

Recently we have become aware of an email scam that attempts to get business managers, finance and operations managers, or parish and school staff to initiate wire transfers.

The request comes in the form of an email that appears to come from a vendor or client with an urgent request to transfer funds or to share financial account information. This type of scam is prevalent on the Internet and is successful because people trust that the request is legitimate. In most cases, the email is being sent from another account but is made to look like it is coming from the client or vendor.

Some simple steps will prevent you from falling victim to this type of scam:

- **Under no circumstances should the transfer of funds be performed solely on the basis of an email exchange.** Emails can easily be spoofed to appear that they are coming from a specific person.
- **Prior to any funds transfer, confirm in person or over the phone the specific instructions to transfer funds**. Do not simply exchange emails; confirmation needs to occur through another means.
- **Do not share account number and banking information over email.**

These scams attempt to create a sense of urgency regarding the need to complete the fund transfer quickly, while also creating the illusion that the person is not available to do it themselves.

If you feel that your financial account information has been compromised, please contact your financial institution immediately; they will know how to address the situation. A 30-second phone call can save your organization thousands of dollars.