Office of Risk Management
RISK ALERT
No. 2021-20

Re: Payroll Diversion Scam **August 9, 2021**

Recently we have become aware of a payroll diversion fraud email scam targeting business managers, finance and operations managers, or parish and school staff.

The scam comes in the form of an email that appears to come from an employee, requesting to internally change their banking information to process a direct deposit of their paycheck. Instead, the paycheck is being stolen by the scammer. This type of scam is prevalent and is successful because people trust that the request is legitimate and comes directly from the employee. In most cases, the email is being sent from another account but is made to look like it is coming from the employee.

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.**

In general, remember to always obtain verbal confirmation whenever a request is made for, or about, money, banking information, or personal information.

If you feel that your financial account information has been compromised, 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. You should additionally contact your payroll provider, the Office of Risk Management, and IT to notify them of the incident.