Ratio Risk Services / RCAB
RISK ALERT
ACCOUNT HACK RISK
No. 2022-39

Re: Fake checks **November 4, 2022**

Recently one of our parishes reported that someone tried to deposit a fake check – which was in the pastor's name – into their own account on behalf of the parish. Luckily, the check, cashed to an address in Ohio, was caught by the bank, who noticed that it did not resemble the usual checks used by the parish.

Although we are more used to cybersecurity risks, it's important to remain vigilant about potential fake check scams. These scams work because fake checks generally look just like real checks, even to bank employees, and are often printed with the names and addresses of legitimate financial institutions. They may even *be* real checks written on bank accounts that belong to someone whose identity was stolen. It can take weeks for a bank to figure out that the check is a fake. According to the FTC, faking checks are one of several ways that perpetrators can commit check fraud. You can read more about other forms of check fraud here.

Be on your guard for unauthorized withdrawals and always take several steps before you respond to any request for payment. Know who has access to the parish checkbook and run all transactions through the parish business managers. Scammers know that once lost, there is usually no way to get your money back.

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

- **Don't rely on money from a check** unless you know and trust the person you're dealing with.
- **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.
- **Frequently check your bank account for possible unauthorized payments**. Check over all charges at least once a week and flag any suspicious or unrecognized charges. Be on the alert for very small amounts that may "test" whether they can follow up with a larger amount, as this is a big red flag.
- **Check with your bank** about controls over unauthorized debits and large, suspicious withdrawals.
- **When in doubt, contact the Office of Risk Management.**

REMEMBER: STOP – CALL – CONFIRM

If you have any questions, please contact us at madeline@ratiorisk.com.