Bank Fraud Alert

July 5, 2022

To: Pastors/Administrators, Parish and School Business Managers/DAS Bookkeepers, Parish Council Finance Chairs and Liaisons

From: Christopher Brown, Chief Financial Officer

In the last two weeks, two of our parishes reported that their bank accounts were compromised. One reported that fake parish checks were created, with the correct bank routing and account numbers on them. The checks were presented at a branch of the parish's bank where they were cashed. Criminals don't need to steal your paper check stock to issue fraudulent checks.

Fraudulent bank transactions are one of the most rapidly growing financial crimes we face. In addition to the lost money, there are other soft and hard costs associated with these crimes:

- Cost of your, and others' time
- Police reports must be filed
- Insurance claims are made
- Opening a new account.
    - New signature cards, and other paperwork
    - Cost of new checks
    - Changing any automated transactions to the new account
    - Reissuing outstanding checks in the old account, from the new account
- Parishioners may be less comfortable making donations if they feel that the funds may end up in the wrong hands because effective financial controls are not in place.

It is time to review financial controls and institute the necessary steps to protect parish and school bank accounts from fraudulent activity. If your bank does not offer appropriate fraud detection tools, it is time to change banks.

- **Monitor Your Account Daily**. Log in to your online banking every morning to check the account(s) for any suspicious activity.

There are fees, which are de minimis, associated with many fraud prevention services, but they are far less than the cost of fraudulent transactions. If you file a claim and Catholic Mutual determines there is coverage, coverage is limited and, at the very least, the deductible is the responsibility of your location. Coverage limits are capped, and you may not recover the full amount of the loss.

The cost of insurance coverage for these crimes is increasing.

Failure to implement fraud detection tools on entity bank accounts could result in insurance premium surcharges for your location.

See page 2 of this document for recommended fraud detection tools to implement with your bank(s).

ARCHDIOCESE of MILWAUKEE

Bank Fraud Alert

Automated fraud detection tools that should be implemented with your bank:

- **Positive Pay**. The process is easy to use, and your bank has staff to walk you through the set-up process. When checks are issued, you download a check register file into the format required by your bank to capture the check date, check number, dollar amount, and we recommend including the payee. This positive pay file is then uploaded to the bank. When a check presents for payment, the information on the check is compared to the positive pay file. If the information matches, the check will clear. If the check is suspect and the information does not match, you will receive a message from the bank and you determine if the check should be paid.

- **ACH Debit Filter (ACH Positive Pay)**. You control the entities that are allowed to electronically withdraw funds from your bank account. You also set limits on the amounts allowed entities can withdraw. If the amount is exceeded, you receive a message from the bank and you then determine whether or not to allow the transaction to be paid.

- **ACH Debit Block.** With a Debit Block no electronic (ACH) debit transactions are allowed.

- **Post No Checks.** If you have an account that is used to accept deposits and make transfers (you have no check stock for this account), you can set up Post No Checks status for the account. This will prevent any check from clearing this account.

Failure to implement fraud detection tools on entity bank accounts could result in insurance premium surcharges for your location.

If you have questions regarding these fraud detection tools, please reach out to your banking representative.

If you have other questions, please contact Kim Kasten at kastenk@archmil.org or 414-769-3326, or me at brownc@archmil.org or 414-769-3325.