ARCHDIOCESE OF BALTIMORE BANK FRAUD PREVENTION POLICY & PROCEDURE	**SECTION** 100 Fiscal Services ~ Internal Control Procedures **SUBSECTION** 111 Bank Fraud Prevention Policy & Procedure

SECTION 111 Bank Fraud Prevention

In recent years, incidents of fraudulent bank transactions have increased significantly. In 2021, 71% of businesses reported being victims of some form of payment fraud, with check fraud alone rising over 300% post-pandemic. Non-profits are particularly targeted as they often lack the sophistication to prevent or detect fraud. Multiple forms of payment fraud were experienced by the Archdiocese of Baltimore parishes and schools at the end of 2022 and the beginning of 2023. To minimize the potential for loss from fraudulent banking transactions, the Board of Financial Administration and the College of Consultors have approved the following policy:

111 Policy ***Positive Pay All parishes and schools within the Archdiocese of Baltimore must implement the Positive Pay system offered by their bank for checks and ACH/Wires for all bank accounts. In addition, they must ensure additional preventive and detective controls are put in place over all bank accounts to minimize the opportunity for loss. Failure to use Positive Pay will increase the Risk Deductible from $2,500 or 25% of the loss (depending on the usage of internal controls) to 50% of the loss.***

Procedures:

Bank/Payment fraud can occur through various methods, including but not limited to:

- Checks stolen from the mail
- Phishing scams
- Vendor impersonation
- Executive impersonation
- Unauthorized online access
- Payroll account change
- Account takeover & mule accounts
- Double deposit (remote and in person)

ARCHDIOCESE OF BALTIMORE BANK FRAUD PREVENTION POLICY & PROCEDURE	**SECTION** 100 Fiscal Services ~ Internal Control Procedures **SUBSECTION** 111 Bank Fraud Prevention Policy & Procedure

To prevent and/or detect the various forms of payment fraud listed above, parishes and schools should implement the following procedures:

No cost office internal controls:

- Deliver mail that includes checks directly to the post office or mail carrier; do not use the blue post office boxes or home mailboxes.
- Limit your bank accounts. Every account adds additional risk.
- Utilize the Archdiocese of Baltimore Payer Express system for insurance premium payments
- Pay through ACH/Wire (push method preferred over pull method) - with dual approval requirements
- Verify payment instructions or changes using Callbacks to known & trusted numbers
- Ensure proper safekeeping of both check stock and checks received, as well as the timely destruction of received checks
- Implement the use of Multi-Factor Authentication for online access to all accounts at financial institutions and/or for systems which hold account information
- Frequently Update Passwords and use strong passwords i.e. passwords that include a number or special character. Additional password best practices include: Never use personal information, use a longer password, don't use the same password on multiple accounts and include Capital letters, numbers and symbols.
- Review bank transactions through the online banking portal several times during the week
- Complete monthly bank reconciliations for each bank account immediately after receiving the statement

Security Software purchased by the Parish Office:

- Antivirus/Malware Prevention Software
- Multi factor authentication software
- VPN software for those who access the Parish system remotely

Restrictions/Controls set up through an FDIC insured bank with fees

- Positive Pay(Recommended/Preferred) & Reverse Positive Pay
    - If you make payments by check add either Positive Pay or Reverse Positive pay

features offered by your bank.
    - If you make payments by ACH – add ACH Positive Pay or equivalent features offered by your bank. If you allow certain business's access to automatically pull payments (not recommended) then you need to add bank features that limit this ability to only approved vendors and always have maximum amounts set that would require manual review and approval if not met.
- Accounts structured with the following limitations:
    - Only receive credits (deposits)
    - Zero balance
    - Tokenization
    - User permissions
- Account validation services
- ACH Credit Block
- Check blocks
- Fraud detection services - prevents transactions to regions or beneficiaries known for fraud

If a bank/payment fraud is detected the parish or school should take the following steps:

1. Notify Bank immediately
    a. Issue stop payments if possible
    b. Try to initiate payment recall
    c. Pull payment audit reports - shows all transactions
    d. Review user audit reports (reports detailing user activity)
2. Notify Law Enforcement
3. Notify AOB Office of Risk Management
4. Notify Regional Controller
5. Change all passwords
6. Update Parish antivirus/malware software
7. Train employees
8. Create new response plan based on what was learned