ANGLICAN DIOCESE OF NIAGARA

Best Practice on Controls to Help Prevent and Detect Email and Other Related Frauds

All diocesan employees should be aware of common BEC (Business Email Compromise) and associated cyber scams and fraud.

To reduce risk, the following strategies should be deployed to authenticate any requests for changes to account information and/or request for payment.

1) **Verify the sender's email** address matches the sender's email address on file; and not just the name displayed in the sender field.
    a. If a business, confirm website and/or contact information is accurate.

2) **Confirm request** using two independent sources of information: an email address and a subsequent phone call or text or in-person conversation.

Additional best practices to reduce the risk of fraud:

- Verify all charges made to diocesan credit cards or accounts to ensure they are business-related on a regular basis.
- Never share one's password or personally identifiable information in response to an email request.
- Keep all software and systems updated.
- Don't over-share personal or organizational information on social media; it could be used to facilitate identity theft and/or impersonating a colleague.

Additional Protocols for Finance Staff

Use a system of checks and balances to ensure no one person controls all parts of a financial transaction.

- Require purchases, payroll, and disbursements to be authorized by a designated person.
- Separate handling (receipt and deposit) functions from record-keeping functions (recording transactions and reconciling accounts).
- Separate purchasing functions from payables functions.

If you discover that the diocese is the victim of an email-related fraudulent incident, immediately contact the executive officer and treasurer.

Cathedral Place
252 James St. N.
Hamilton, ON L8R 2L3

905-527-1316
niagaraanglican.ca