Catholic Diocese of Columbus

■ Policy ☐ Guideline

☐ Diocesan ☐ Parish ☐ School ■ All

601.3 Verification for Payment changes and purchases

The Diocese of Columbus has established a policy to require that all requests received via e-mail, text or voice (phone calls and voice-mail messages) for changes to payment information, and for purchases must be validated through a separate known channel. These are required to prevent theft of funds that can impact the diocese, parishes, schools, and even individuals. Each of these are explained in more detail below.

Impersonation through e-mail, text, and voice methods

These impersonation requests can come through various means including phone calls, text messages, e-mails, or physical mail. Thieves continuously improve their techniques to convincingly impersonate others, and often use a combination of channels (such as e-mail and phone). In the past, these were often easier to spot through poor spelling, poor use of language and other clues. Thieves are becoming increasingly hard to detect, and now use tools like Artificial Intelligence to create a very convincing impersonation including simulating someone's voice in a phone call. Actual examples have included e-mails with the sender address disguised to look like a vendor, employee, priest, principal, director, and even the Bishop.

Payment change requests

Criminals frequently impersonate to request a change to the method of payment, such as a vendor or employee asking that their bank account be changed. Actual examples have been requests to change an employee's bank account to steal their paycheck, and a vendor request to change their bank account to steal an up-coming payment. It's important to note that these requests sometimes come from the legitimate e-mail, text, or phone of the person being impersonated after a hacker broke into their account – making the request appear fully legitimate.

Purchase Requests

Impersonators may ask for you to conduct a financial transaction on their behalf. Recently a priest was impersonated by e-mail and text to request a staff member purchase gift cards to reward other staff. Most commonly these requests are for gift cards that are easily and quickly used – such as to Amazon or another major retailer. These requests nearly always are requesting a favor and communicate urgency and short timelines – to get you to suspend caution and respond before you think twice. These requests usually are impersonating an authority, such as your manager (or higher), your priest, your Principal – with the hope you will be too nervous to question or challenge them. It's critical that the most important people are also the most frequently impersonated. The more important "the requester" is, the more suspicious you need to be.

The Requirement for Validation

The policy requires that these requests be validated – and through a separate previously known channel – to verify the requester is not being impersonated. "Separate previously known channel" means that you connect with the request or through a different method (phone, text, e-mail, etc.) than how they made the request, and that you DO NOT rely on contact information in the request. For example, if you get an e-mail with the request and includes a phone number to call them back, do not use that phone number! Call or text them with a number you already know to verify the request.