Archdiocese of St. Louis Identity Theft Protection Policy

Many parishes, schools and agencies of the Archdiocese of St. Louis collect personal information about persons whom they serve. Examples of personal information include social security numbers, address information or credit card information (collectively, "Personal Information"). This Personal Information may be collected when a parent enrolls a child in a parish school, when a parent enrolls a child for an athletic event, when a person is seen at a counseling center or when a person makes a deferred payment for a service, such as purchasing a pre-paid burial plot. Additionally, Personal Information may be collected about persons who participate in the Safe Environment Program of the Archdiocese. In collecting and maintaining such Personal Information, parishes (included parish organizations, such as Athletic Associations), schools (including pre-school and after-school-care programs) and agencies of the Archdiocese MUST work to ensure that identity theft is detected, prevented, and mitigated.

In order to respond to potential threats of identity theft, all parishes (including parish organizations, such as Athletic Associations), schools (including pre-school and after-school-care programs) and agencies that collect Personal Information are required to:

1. Have a process in place to verify a person's Personal Information, if the organization believes that information furnished by an individual may be fraudulent. This process could involve asking for proof of identification or additional information or verifying previously collected information maintained by the organization.

2. Maintain physical safeguards to ensure that collected Personal Information is securely maintained. This may include locking file cabinets where Personal Information is stored and allowing only certain persons within the organization to access Personal Information. Additionally, Personal Information should NOT be removed from the parish, school or agency and stored in an employee's or volunteer's home or personal office.

3. Maintain technical safeguards, if the Personal Information is stored electronically. This should include having electronically stored Personal Information protected by passwords which are periodically updated and are not shared with others. Laptop and notebook computers, personal digital assistants (PDAs), cell phones, zip drives and other portable devices should NOT be used to store Personal Information.

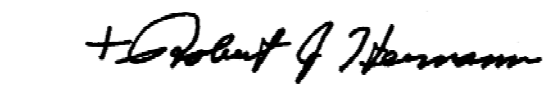
4. Respond to information that appears to be inconsistent with information previously maintained about an individual. This could include verifying a discrepancy in address information.

5. Notifying persons whose Personal Information may have been compromised. If a parish, school or agency believes that Personal Information has been compromised, it must contact the pastor or agency director, who shall assist in this notification and determine whether to involve Archdiocesan officials and law enforcement.

6. Identify a representative of the parish, school or agency responsible for ensuring that identity theft prevention procedures are maintained and followed.

In addition to these six requirements, parishes, schools and agencies are expected to understand and identify areas of vulnerability which may result in identity theft of Personal Information and further protect Personal Information as their specific operations necessitate.

This policy shall be updated periodically to ensure that parishes, schools and agencies of the Archdiocese are properly addressing the risk of identity theft of Personal Information.



Most Reverend Robert J. Hermann
Archdiocesan Administrator

May 27, 2009