



ARCHDIOCESE OF PORTLAND

IN OREGON

c/o ID Experts
10300 SW Greenburg Rd, Ste 570
Portland, OR 97223

July 28, 2014

[Full Name]
[Address]
[City], [State] [Zip]

Dear [First Name],

As you may know, the security of personal information of volunteers and employees of the Archdiocese of Portland, parishes, and schools has been compromised in a national tax fraud scheme. I am writing because you notified us that you were a victim in this scheme, and we confirmed that you provided your Social Security number, for purposes of employment or volunteer service, to a parish, school or other entity for which the Archdiocese oversees background checks. Please accept my sincerest apologies for any anxiety and inconvenience these events and circumstances may have caused you.

Generally, an organization that owns, maintains, or otherwise possesses personal information notifies individuals in the event the organization determines that it has suffered a security breach that compromised personal information. Despite all our efforts, we have not determined how your personal information was compromised and whether the security breach occurred within the Archdiocese's systems/records or those of another. Nonetheless, we want to tell you what we know and provide you with some important information about steps we are taking to help protect you in the future, including offering free credit monitoring services.

What happened?

Starting in mid-March 2014, we learned that a number of individuals affiliated with our Archdiocese (mostly employees and volunteers at parishes and schools) had been victimized in a tax fraud scheme. Based on the information provided by affected individuals, it appears that criminals obtained their social security numbers and filed false tax returns using their identities in an effort to obtain fraudulent refunds.

We have been hard at work trying to determine the cause of this breach and how it occurred. Unfortunately, at this time we still do not know:

- who compromised the personal information, and how it was done;
- whether any personal information, other than names and Social Security numbers, was compromised;
- whether the breach occurred within our systems or the systems of another; and

- the identities of individuals whose personal information was compromised by the breach (unless they have notified us directly).

What are we doing about it?

Since first learning of this situation, we have worked with law enforcement, including the IRS and FBI, and hired a national forensic firm all in an effort to determine the source of this breach. We have worked with third parties with whom we contract to determine if the breach took place in their systems. We have also gathered information from victims to assist with the investigation, and communicated by telephone, through our website, and otherwise to help them understand what was happening and what steps they could take to protect themselves. Finally, we are reviewing our systems, policies, and procedures for handling personal information, to enhance the overall security of personal information we receive.

What will we do for you?

In an effort to help protect you, we have arranged for you to enroll, at no cost, in an online three bureau credit monitoring service (*MyTransUnion Monitoring*) for two years provided by TransUnion, one of the three nationwide credit reporting companies. Due to privacy laws, we are not able to enroll you directly. For more information on *MyTransUnion Monitoring* and instructions on how to activate your free two-year membership, please see the enclosure with this letter.

What further action should you take?

Please remain vigilant by carefully reviewing your account statements and monitoring your free credit reports.

If you have not already done so, you should notify the IRS Identity Protection Specialized Unit (open, Monday – Friday 7 a.m. – 7 p.m.) at 1-800-908-4490. The IRS tells us that, due to the volume of calls it receives, it may not respond to you directly unless it requires more information from you; also that its voicemail box becomes full on occasion. The IRS says it is doing everything it can to listen to the voicemails in a timely manner and process information it receives.

You may also consider contacting one of the major credit bureaus listed below to place a fraud alert or security freeze on your credit reports:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 680-7289
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

We also strongly encourage you to report suspected incidents of identity theft to law enforcement, including the Federal Trade Commission at 1-877-ID-THEFT (1-877-438-4338) or at Federal Trade Commission - Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. If you want to learn more about how to avoid identity theft, please visit the U.S. government's identity theft information website, <http://www.consumer.gov/idtheft>.

We have been advised that in the aftermath of security breaches such as this, some criminals seek to fraudulently obtain the personal information of affected individuals by claiming to be the business

experiencing the breach. **Do NOT respond to any e-mails or other requests from entities requesting your sensitive personal information in relation to this breach. The Archdiocese of Portland will NOT ask you for your sensitive personal information.** If you receive any written or electronic request via e-mail purporting to be from the Archdiocese of Portland and it looks suspicious, please contact us immediately, at the number referenced below:

You will find additional information about this tax fraud matter on our website, www.archdpx.org. As we learn more, we are updating these pages. You may also contact us by email at: taxinformation@archdpx.org, or telephone at: 1-888-472-9740 or 503-416-3475 with your tax fraud questions.

We understand how concerned you were upon learning you were victimized in a tax fraud scheme. I share that concern. The security of our employees' and volunteers' personal information is a high priority. Please be assured that we continue to explore ways to enhance the security of your personal information.

You are in my prayer, especially during this stressful time.

Sincerely in Christ,

A handwritten signature in blue ink, appearing to read "Alexander K. Sample".

Most Rev. Alexander K. Sample
Archbishop of Portland in Oregon

Encl: *TransUnion Monitoring Enrollment Information*



ARCHDIOCESE OF PORTLAND

IN OREGON

TransUnion Monitoring Enrollment Information

1. You Must Enroll By: **September 30, 2014**
2. TransUnion Monitoring Website: www.transunionmonitoring.com
3. Your Activation Code: **[Insert Unique 12-letter Activation Code]**

To enroll in this service, at no cost to you, go to the TransUnion Monitoring website at www.transunionmonitoring.com and in the space referenced as "Activation Code," enter the following unique 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the simple three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet, as an alternative, you may enroll in a similar offline paper based three-bureau credit monitoring service, via U.S. Mail delivery, by calling the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422** and when prompted, enter the following 6-digit telephone pass code: **745148**.

You can sign up for the online or offline credit monitoring service anytime between now and **September 30, 2014**. Due to privacy laws, we cannot register you directly.

Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number.

Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more.

The service also includes up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)