David D. Axtell
612.335.7247 **DIRECT**
612.335.1657 **DIRECT FAX**
david.axtell@stinson.com

STINSON
LEONARD
STREET

October 5, 2017

VIA FEDERAL EXPRESS

Attorney General Gordon MacDonald
Consumer Protection and Antitrust Bureau
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Data Breach Notification: Catholic United Financial: NAIC #57053

To Whom It May Concern:

This firm represents Catholic United Financial, a Minnesota domiciled fraternal benefit society, located at 3499 Lexington Avenue North, St. Paul, Minnesota 55126. Catholic United Financial is not licensed to transact insurance in New Hampshire, but has members who now reside in your state following their policy having been lawfully issued in a state where the Company is licensed.

On September 6, 2017, Catholic United Financial became suspicious that there may have been an attack on its web server and was concerned that such an attack may have led to the unauthorized access to personally identifiable information of Catholic United Financial's members. On that same day, Catholic United Financial hired outside forensic investigators to assess the situation and determine whether such a breach had occurred. Catholic United Financial immediately removed all potential access to personally identifiable information on its web server and secured the web server from any possible further attack.

On September 20, 2017, the forensic investigator issued its final report which concluded that Catholic United Financial's web server had been subjected to SQL injection attacks by an unknown person(s). The forensic investigator further found that Catholic United Financial's web server experienced unusually high traffic on July 31, and August 26, 27, and 28 of this year, consistent with an attack. Further analysis revealed that SQL injection attacks also occurred prior to those dates, and that such attacks may have allowed unauthorized access by attackers to personally identifiable information of Catholic United Financial members as of November 12, 2016, when member social security numbers were uploaded to the web server. At this time, Catholic United Financial believes that 39 individuals who provided it with New Hampshire addresses (including the deceased and those that did not potentially have their social security numbers exposed), may have had their data compromised.

In response to this attack, Catholic United Financial has notified local law enforcement as well as the FBI, and is cooperating in their investigations. Catholic United Financial is also

hardening its security with the help of outside experts to ensure similar attacks cannot be successful in the future.

Catholic United Financial will be providing written notification to all of its members, whether impacted by potential exposure of their social security numbers or not. It will also be notifying family members of its deceased members who may have had their personal information compromised. Presently the notices are planned to be mailed to consumers on October 6, 2017. There are several slight variants on the notice letter depending on the recipient (e.g., whether their social security number was compromised or not, whether they are deceased, whether they are minors, and to comply with particular disclosure requirements in a specific state). We are attaching a sample copy of the notification letter that will go out to living members who had their social security number potentially compromised.

In conjunction with KROLL, a nationally known data security and breach notification firm, Catholic United Financial will provide guidance to all of its current and former members regarding the breach and how to protect themselves from possible identity theft. Catholic United Financial is offering through KROLL and free to all those notified: 24 months of credit monitoring, fraud consultation, and identity theft restoration for all living adults; fraud consultation and identity theft restoration for a year in relation to the deceased; and for minors, minor identity monitoring, fraud consultation, and identity theft restoration for a year.

Catholic United Financial takes this matter very seriously both as a victim and as an institution dedicated to its members. If you require any additional information beyond what is provided in this letter, please contact me directly.

Sincerely,
Stinson Leonard Street LLP

David D. Axtell

cc: Harald Borrmann,
Chief Executive Officer
Catholic United Financial

Catholic United Financial

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

Since 1878, Catholic United Financial has been your trusted partner in helping you manage your personal finances and in contributing to the financial well-being of our Catholic communities. We have earned your trust in those 139 years. It is with that in mind that we are letting you know that third-party criminal activity may have allowed unauthorized access to some of our members' personal information. While the finances of our Association were never at risk, some member personal information may have been compromised. Within one day of our becoming aware that such an incident may have occurred, we took action to completely shut down our website, thus closing off any future attempts at such illegal activity. We also immediately hired an outside forensic team to investigate what may have occurred and the member data that may have been accessed. We are now restoring our website with even-more enhanced security measures and programming. I want you to know that we take our responsibilities as your financial partner extremely seriously, and our response to this incident will demonstrate our strong commitment to our members. Please read the notice below; we look forward to assisting you as we respond to this intrusive action.

What happened?

On September 6, 2017, Catholic United Financial became suspicious that there may have been an intrusion on its web server and was concerned that such an intrusion may have led to the unauthorized access to personally identifiable information of Catholic United Financial's members. On that same day, Catholic United Financial hired outside forensic investigators to assess the situation and determine whether such an intrusion had occurred. Catholic United Financial immediately removed all potential access to personally identifiable information on its web server and secured the web server from any possible further intrusion.

On September 20, 2017, the forensic investigator issued its final report which concluded that Catholic United Financial's web server had been subjected to SQL injection attacks by an unknown person(s). Such attacks may have allowed unauthorized access by attackers to certain personally identifiable information of Catholic United Financial members as of November 12, 2016. We estimate that approximately 127,310 current and former members, whose on-file addresses indicate they live in a variety of locations including in your state, may have had their personal information containing Social Security numbers accessed, including approximately 7,356 deceased members. Out of an abundance of caution we are notifying all current and former members including the families of the deceased and those that did not have their Social Security numbers potentially compromised and offering all of them the identity monitoring detailed in this letter.

In response to this incident, Catholic United Financial has notified the Ramsey County, Minnesota sheriff as well as the FBI, and is cooperating in their investigations. This notice was not delayed at the request of law enforcement.

What information was involved?

Our records indicate that member first names, last names, mailing addresses, dates of birth, email addresses, insurance policy information, and Social Security numbers were potentially accessed by unauthorized individuals. Other information, such as your beneficiary information and login credentials were not accessed.

What we are doing.

Catholic United Financial is hardening its security with the help of outside experts to ensure similar intrusions cannot be successful in the future. Online services are being restored only after such hardening has been completed for that service. At this time, Catholic United Financial has not yet determined its own time and cost required to rectify this situation, but is committed to providing you with the information and services stated in this letter.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **February 8, 2018** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-202-7414. Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. Should you become the victim of identity theft, or if you would like more information regarding how to protect yourself from identity theft, we encourage you to visit the FTC's identity theft website at https://www.identitytheft.gov/.

For more information.

If you have questions, please call 1-833-202-7414, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. I sincerely apologize for any inconvenience this may cause you. Nothing is more important to us than our members. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Harald E. Borrmann

President, CEO, and Chair of the Board
Catholic United Financial
3499 Lexington Avenue North, St. Paul, Minnesota 55126
1-800-568-6670

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111; Fraud Division: 1-800-525-6285

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213; Fraud Division: 1-800-680-7289

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumerftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. You may contact any of the above credit reporting agencies or the Federal Trade Commission for more information on how to place a fraud alert.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.) For more information on placing a security freeze, you may contact any of the above credit reporting agencies or the Federal Trade Commission.

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, Rhode Island 02903, http://www.riag.ri.gov, consumers@riag.ri.gov, 1-401-274-4400.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report.

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.