



A business advisory and advocacy law firm®

Nicholas A. Kurk
Direct Dial: 312-642-6738
E-mail: nkurk@mcdonaldhopkins.com



McDonald Hopkins LLC
300 N. LaSalle Street
Suite 1400
Chicago, IL 60654

P 1.312.280.0111
F 1.312.280.8232

February 3, 2023

VIA U.S. MAIL

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: RBC Ministries dba Our Daily Bread Ministries – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents RBC Ministries dba Our Daily Bread Ministries (“ODB”). ODB is a Michigan nonprofit corporation and serves as a global ministry with a mission to make the life-changing wisdom of the Bible understandable and accessible to all.

I am writing to provide notification of an incident at ODB that may affect the security of personal information of approximately 256 Maryland residents. Although ODB’s investigation is complete, this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, ODB does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

ODB experienced an unauthorized third-party intrusion into its e-commerce website page during the period of November 18th through December 29th, 2022. Upon learning of an issue, ODB immediately commenced a prompt and thorough investigation, which included working very closely with external cybersecurity professionals experienced in handling these types of incidents. On or around January 4, 2023, ODB’s extensive forensic investigation has led it to believe that the website intrusion may have allowed an unauthorized third party to access and/or acquire some personal information, including names, addresses, emails, telephone numbers, and credit card information. As ODB does not collect Social Security numbers or other personal information than listed here, that information was **not** accessed and/or acquired.

Out of an abundance of caution, ODB wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. ODB will be providing the affected residents with written notification of this incident commencing on or about February 3, 2023 in substantially the same form as the letter attached hereto. ODB is advising the affected residents about the process for placing fraud alerts

Page 2

and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Federal Trade Commission, and the Maryland Attorney General.

At ODB, protecting the privacy of personal information is a top priority. ODB remains fully committed to maintaining the privacy of personal information in its possession and has taken multiple additional precautions to safeguard it. ODB continually evaluates and modifies its practices to enhance the security and privacy of personal information.

If you have any additional questions, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'N. A. Kurk', with a stylized, cursive script.

Nicholas A. Kurk

Encl.



Our Daily Bread
Ministries

***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

Dear [REDACTED]

For 85 years, Our Daily Bread Ministries' mission has been to make the life-changing wisdom of the Bible understandable and accessible to all. Thank you for coming alongside us in that mission. The privacy and security of the personal information we maintain is of the utmost importance to Our Daily Bread Ministries. We are writing to you today with important information regarding a recent data security incident that may have involved some of your information. We wanted to make you aware of this incident and assure you that significant measures are being taken to protect your personal information.

What Happened?

We experienced an unauthorized third-party intrusion into our e-commerce website page during the period of November 18th through December 29th, 2022.

What We Are Doing

Upon learning of an issue, we immediately commenced a prompt and thorough investigation, which included working very closely with external cybersecurity professionals experienced in handling these types of incidents. On or around January 4, 2023, our extensive forensic investigation led us to believe that the website intrusion may have allowed an unauthorized third party to access and/or acquire some of your personal information. Our forensic investigation is now complete.

What Information Was Involved?

During the unauthorized intrusion, the third party may have accessed and/or acquired your name, address, email, telephone number, and credit card information. As we do not collect your Social Security number or other personal information than listed here, that information was not accessed and/or acquired.

What You Can Do

Out of an abundance of caution, we wanted to make you aware of the incident. This letter provides precautionary measures you can take to protect your personal information, including canceling and replacing the credit or debit card used with us, placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies for any inconvenience that this incident has caused. We remain fully committed to maintaining the privacy of personal information in our possession and have taken multiple additional precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information. Your partnership with us is critical to the ministry work we do. Thank you for your prayers and working with us through this unfortunate attack on the ministry.

If you have any further questions regarding this incident, please contact us at [REDACTED] or via email at [REDACTED]

Sincerely,

Our Daily Bread Ministries

[REDACTED]

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.