McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248.220.1354
jgiszczak@mcdonaldhopkins.com

March 28, 2014

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: LOGOS Management Software, LLC – Incident Notification

Dear Attorney General Delaney:

We represent LOGOS Management Software, LLC ("LOGOS") and are writing to notify you of a data privacy incident that may affect the security of personal information of three (3) New Hampshire residents. LOGOS' investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission. By providing this notice, LOGOS does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

LOGOS is the online giving and profile provider for parishes throughout the country. On or about February 4, 2014, LOGOS was informed by a donor that there was a possible unauthorized transaction on the donor's credit card. Upon learning of the incident, LOGOS immediately commenced an investigation, retained a third-party computer forensic company to analyze the extent of the unauthorized activity and reported the incident to law enforcement.

Based on information discovered to date, LOGOS knows that the server owned by the third-party service company that hosts a component of the Ministry Connect system used for electronic donations was accessed by an unauthorized intruder. The nature of the compromise affected profile and/or payment information for new or changed gifts that were entered into the system from Friday, January 17, 2014 through Tuesday, February 4, 2014. The Ministry Connect service was restored on February 23, 2014.

Since completing the forensic investigation, LOGOS has devoted considerable time and effort to determine what exact information may have been affected as a result of the incident. LOGOS can confirm that full names, together with either credit card or bank account information (routing and checking numbers), depending on the form of payment that was used to make a donation in the Ministry Connect system, was contained on the compromised server.

We wanted to make you (and the affected residents) aware of the incident and explain the steps LOGOS is taking to safeguard residents against identity fraud. LOGOS provided the New Hampshire residents with written notice of this incident on March 27, 2014, in substantially the same form as the letter attached hereto. LOGOS has advised the residents to monitor all credit reports and bank statements and to contact their banking institution or credit card company if they notice any suspicious activity. LOGOS has offered a complimentary one-year membership in Experian's® ProtectMyID® to all affected residents. LOGOS is also providing call center support for those affected. LOGOS also advised the individuals affected to obtain a credit report and the process for placing a fraud alert on their credit files.

Maintaining the privacy of personal information is of the utmost importance to LOGOS. In light of this incident, LOGOS has taken action to protect its customers, donors and its own servers from further harm. LOGOS has closed all access to the server by the unauthorized party. In addition, LOGOS has relocated the Ministry Connect system to a server which it owns and manages. Moreover, LOGOS has conducted a full analysis of all of its servers to confirm their integrity from external threats.

Should you have any questions regarding this notification or the incident, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,

James J. Giszczak

JJG/dap
Encl.

LOGOS
Powering Your Ministry

<Date>

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

<FirstName> <LastName>
<Address1>
<Address2>
<City>, <State> <ZIP>

Dear <FirstName> <LastName>:

I am writing to follow-up on a security incident that was previously brought to your attention, potentially involving your personal information. LOGOS is the online giving and profile provider for <PARISH>. On or about February 4, 2014, LOGOS was informed by a donor that there was a possible unauthorized transaction on the donor's credit card. Upon learning of the incident, we immediately commenced an investigation, retained a third-party computer forensic company to analyze the extent of the unauthorized activity and reported the incident to law enforcement.

Based on information discovered to date, we know that the server owned by the third-party service company that hosts a component of the Ministry Connect system used for electronic donations was accessed by an unauthorized intruder. The nature of the compromise affected profile and/or payment information for new or changed gifts that were entered into the system from Friday, January 17, 2014 through Tuesday, February 4, 2014.

Since completing the forensic investigation, we have devoted considerable time and effort to determine what exact information may have been affected as a result of the incident. We can confirm that your full name, together with either your credit card or bank account information (routing and checking numbers), depending on the form of payment that you used to make a donation in the Ministry Connect system, was contained on the compromised server. We want to make you aware of the incident and explain the steps we are taking to safeguard you against identity fraud and suggest steps that you should take as well.

In light of this incident, LOGOS has taken action to protect our customers, donors and our own servers from further harm. We have closed all access to the server by the unauthorized party. In addition, we have relocated the Ministry Connect system to a server which we own and manage. The Ministry Connect service was restored on February 23, 2014. Moreover, we have conducted a full analysis of all of our servers to confirm their integrity from external threats.

LOGOS takes this situation very seriously. We deeply regret that your personal information was involved in this incident. Maintaining the integrity of your confidential information is of the utmost importance to us. Enclosed you will find information on enrolling in a complimentary 12-month credit monitoring service along with other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and obtaining a free credit report. If you have not done so already, we advise you to please call your banking institution to determine if you should change your bank account number or contact your credit card issuing bank to inquire about canceling your card. In addition, we encourage you to carefully review your credit reports and financial statements for fraudulent activity.

If you have any further questions regarding this incident, please contact our Customer Support Center at (877) 995-6467 or *customerinfo@logoscms.com*.

Sincerely,

William Pressprich
President & CEO
LOGOS

1. Enrolling in Complimentary 12-Month Credit Monitoring

Protecting your personal information is important to LOGOS. In response to this security incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE that you enroll by **June 30, 2014**.
2. VISIT the ProtectMyID Web Site to enroll: **www.protectmyid.com/redeem**
3. PROVIDE your 9-character Activation Code: <XXXXXXXXX>

If you have questions or need an alternative to enrolling online, please call 877-371-7902.

Additional Details Regarding Your 12-Month ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.)

If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902.

2. Placing a Fraud Alert

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files. 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.

TransUnion	**Experian**	**Equifax**
Consumer Fraud Division	Consumer Fraud Division	Consumer Fraud Division
PO Box 6790	PO Box 9554	PO Box 740256
Fullerton, CA 92834-6790	Allen, TX 75013	Atlanta, GA 30374-0256
www.transunion.com/fraud	www.experian.com	www.equifax.com
1-800-680-7289	1-888-397-3742	1-800-525-6285

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 report online at **www.annualcreditreport.com**.

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 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.