CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

CAROLYN PURWIN RYAN
cpurwin@c-wlaw.com

Admitted in PA and NJ

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

July 9, 2020

Via Mail
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03302

RE: Security Incident Notification

To Whom It May Concern:

I serve as counsel for the National Catholic Educational Association ("NCEA"), and provide this notification to you of a recent data security incident suffered by NCEA. On May 13, 2020, NCEA became aware of a vulnerability to iMIS, NCEA's management software. Upon discovery, NCEA swiftly took steps to secure the iMIS software which includes updating iMIS to remove the vulnerability. Further, NCEA promptly began investigating the vulnerability. NCEA's investigation identified that an unknown individual utilized the vulnerability to add malicious code to the iMIS software that acted as a credit card skimmer between April 10, 2020 and May 18, 2020. As a result, the malicious code may have allowed an unauthorized individual to collect credit card data from transactions that occurred within this time period. Importantly, the vulnerability, as well as the malicious code, has been removed. NCEA has identified one (1) New Hampshire resident potentially impacted as a result of this incident.

NCEA will be promptly notifying the affected individuals on July 9, 2020 and is providing them with complimentary credit monitoring one (1) year. A copy of the drafted letter is attached. As the letter indicates NCEA will be offering credit monitoring and identity restoration services at NCEA's expense. NCEA is taking steps to comply with all applicable notification obligations.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: Carolyn Ryan
Carolyn Purwin Ryan

National Catholic Educational Association
1005 North Glebe Road, Suite 525
Arlington, VA 22201

<<First Name>> <<Last Name >>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>> <<Date>>
<<Country>>

RE: Important Security Notification. Please read this entire letter.

Dear Sir or Madam:

I am writing to inform you of a data security incident experienced by the National Catholic Educational Association ("NCEA") that may have involved your personal information described below.

At NCEA, we take the privacy and security of all information very seriously. While we have no evidence to suggest that any of the impacted information was viewed or misused during this compromise, it is crucial that we be as supportive and transparent as possible. That is why I am writing to inform you of this incident, to offer information about steps that can be taken to help protect your information, and to let you know about complimentary credit monitoring services that we are offering you through TransUnion, one of the three nationwide credit reporting companies.

I sincerely apologize for any concern that this incident may cause you. Let me reassure you that NCEA is fully committed to supporting you.

What Happened:

On May 13, 2020, NCEA became aware of a vulnerability to iMIS, NCEA's management software. Upon discovery, NCEA swiftly took steps to secure the iMIS software which includes updating iMIS to remove the vulnerability. Further, NCEA promptly began investigating the vulnerability. NCEA's investigation identified that an unknown individual utilized the vulnerability to add malicious code to the iMIS software that acted as a credit card skimmer between April 10, 2020 and May 18, 2020. As a result, the malicious code may have allowed an unauthorized individual to collect credit card data from transactions that occurred within this time period. Importantly, the vulnerability, as well as the malicious code, has been removed.

While we have no reason to believe that any information was actually viewed or misused during this compromise, we are providing this notification to you out of an abundance of caution and so that you may diligently monitor your personal information and resources. We take great care in the security of our technology systems, and regret that this incident has occurred.

What Information Was Involved:

It is important to note, as mentioned above, that there is no evidence to suggest that any personally identifiable information has been viewed or misused. The personal information that could have been viewed by the unauthorized individual(s) may have included your first and last name, in combination with your name, address and credit card information utilized in your recent transaction with NCEA.

What We Are Doing:

NCEA has taken every step necessary to address the incident and is committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately began investigating the vulnerability and took steps secure the iMIS software. Additionally, we are offering you complimentary credit monitoring and identity protection services.

Credit Monitoring:

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. Due to privacy laws, we cannot register you directly. Additional information regarding how to enroll in the complimentary credit monitoring service is enclosed.

What You Can Do:

In addition to enrolling in the complimentary credit monitoring service detailed within, we recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 1800-711-6232.

NCEA has no relationship more important or more meaningful than the one we share with you. I want to personally express my deepest regret for any worry or inconvenience that this incident may cause you.

Sincerely,

John R. Reyes, Ed.D.
Executive Director of Operational Vitality
National Catholic Educational Association

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

TransUnion® *my*TrueIdentity provides you with the following key features:

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- One year of unlimited access to your TransUnion® credit report and credit score.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible.[1]

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **October 31, 2020**. 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. Enrolling in this service will not affect your credit score.

➢ PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion	**Experian**	**Equifax**
Fraud Victim Assistance Dept.	National Consumer Assistance	Consumer Fraud Division
P.O. Box 6790	P.O. Box 1017	P.O. Box 105069
Fullerton, CA 92834	Allen, TX 75013	Atlanta, GA 30348
1-800-680-8289	1-888-397-3742	1-800-525-6285
www.transunion.com	www.experian.com	www.equifax.com

➢ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your

[1] (Policy limitations and exclusions may apply.)

credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. You should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. The process to place a security freeze requires that you directly contact each of the credit reporting companies. You can do so online or through the mail. The necessary types of information include your full name, social security number, date of birth, current address, all addresses where you have lived during the last two years, email address, a copy of a utility bill, bank or insurance statement and a copy of a government-issued id card, such as a driver's license or state id card.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. 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.

- **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements.
Be proactive and create alerts on credit cards and bank accounts to notify you of activity.
If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE**

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

- **RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)**

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate,

incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit "prescreened" offers of credit an insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at http://www.annualcreditreport.com.

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.

- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.

- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

- **For New York residents,** you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotectionl; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

- **For Rhode Island Residents,** the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov or 401-274-4400.