MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Christopher J. DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

October 26, 2018

INTENDED FOR ADDRESSEE(S) ONLY
VIA US MAIL ONLY

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Jewish Federation of Cincinnati
File No. 18-08286

Dear Mr. MacDonald:

Our office continues to represent Jewish Federation of Cincinnati ("JFC") located at 8499 Ridge Road, Cincinnati, Ohio. We write to retract our July 9, 2018 notice to your office ("July 9 Notice"), a copy of which is attached as **Exhibit AA.** By providing this supplemental notice, JFC does not waive any rights or defenses regarding the applicability of New Hampshire law, applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Since providing the initial notice, JFC continued its investigation into the incident and its efforts to identify all affected individuals. While JFC's IT department initially believed that the involved laptops were missing hard drives, the organization recently confirmed that the involved laptops actually used solid-state drives which were always safely in JFC's possession, so no data or personal information was ever lost or compromised in any way. As such, there was no breach of security or compromise of personal information and there will not be any additional notification letters sent as previously communicated. JFC apologizes for any unnecessary confusion this may have caused.

We kindly ask that you acknowledge receipt of this letter. If convenient, please send an email to Chris DiIenno at cdiienno@mullen.law.

JFC will continue to offer credit monitoring services for one (1) year, through Kroll, to individuals who were notified, at no cost to these individuals, even though their personal information was never at risk.

Contact Information

Should you have any questions regarding this letter, please contact us at 267-930-4775. We welcome the opportunity to discuss this matter in more detail with you at any time.

Very truly yours,

Christopher DiIenno of
MULLEN COUGHLIN LLC

CJD:aa
Enclosure

EXHIBIT AA

Christopher J. Dilenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

July 9, 2018

VIA U.S. MAIL

Attorney General of New Hampshire
New Hampshire Department of Justice
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Sir or Madam:

We represent the Jewish Federation of Cincinnati ("JFC") headquartered at 8499 Ridge Road, Cincinnati, OH 45236 and are writing to notify your office of an incident that may affect the security of personal information relating to one (1) New Hampshire resident. By providing this notice, the JFC does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

Starting on or about May 14, 2018, the Jewish Federation of Cincinnati learned that one of its employees, who oversees payables and payroll, had two hard drives stolen from her company laptop computer by unknown person(s) while outside the office premises. The thefts were reported to police, but the hard drives were not recovered. JFC immediately launched an investigation and retained a third party forensic investigator to determine the nature and scope of the contents of the stolen hard drives and identify what, if any, personal information was contained on the drives. Backups of the hard drives were data mined to identify the affected individuals, and that investigation is ongoing.

The hard drives contained information concerning payroll and vendor processing including name, address, and social security number. To date, JFC has no evidence of any misuse of the personal information present on the stolen hard drives.

Notice to New Hampshire Residents

On July 9, 2018, JFC provided written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and to Be Taken

Upon discovering the hard drives had been stolen, JFC moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

JFC has security measures in place to protect data in their care and are working diligently to enhance these protections and the security of their systems and physical equipment. JFC reported this incident to law enforcement and to state regulators, where required by law. JFC also provided affected individuals with information about the event and about the steps affected individuals can take to better protect against misuse of their personal information.

As an added precaution, JFC also offered affected individuals access to one (1) year of credit monitoring and identity theft restoration services through Kroll at no cost to the individual. The cost of this service will be paid for by JFC. Individuals were encouraged to enroll in these services.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4775.

Very truly yours,

Christopher DiIenno of
MULLEN COUGHLIN LLC

EXHIBIT A

SHARED
BUSINESS SERVICES
STRENGTH IN NUMBERS

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

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

Re: Notice of Data Breach

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

The Jewish Federation of Cincinnati ("JFC") writes on behalf of <<ClientDef1(Entity Name)>> regarding a recent data security incident that may impact your personal information. The JFC assists <<ClientDef1(Entity Name)>> with the administration of various business functions, including payroll and vendor payment processing, through its Shared Business Services. The JFC recently made <<ClientDef1(Entity Name)>> aware of this security incident. The JFC is providing you with notice of the steps we are taking in response to this incident as well as steps you can take to protect your personal information should you feel it is appropriate to do so.

What Happened

Starting on or about May 14, 2018, the JFC discovered that two hard drives were stolen from an employee's laptop computer. The thefts were reported to the police and their investigation is ongoing. Much of the information stored on the hard drives is related to the JFC's Shared Business Services' clients.

What Information Was Involved

The JFC cannot confirm if your information was actually accessed on the stolen hard drives. However, it was determined that the following information about you was accessible on the hard drives: <<ClientDef2(Breach Details Variable Text)>>

The JFC is not aware of any actual or attempted misuse of your information.

What We are Doing

Upon discovering the theft, the JFC immediately began investigating this incident. The JFC performed a thorough internal investigation and retained the services of outside forensic investigator to determine the full nature and scope of the incident. Due to the nature of investigations, it has taken some time to identify those that may have been affected by this incident.

While the JFC has no indication that any fraud has or will result from this incident, we take the security of personal information in our care very seriously. We have security measures in place to protect the data on our systems and we are working to implement additional safeguards and employee training in response to this incident. For instance, the JFC's accounting department has updated its operating systems and begun using encryption software to provide an added layer of security.

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 one year. 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, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

You have until October 12, 2018 to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

What You Can Do

In addition to enrolling in Identity Theft Protection and credit file monitoring, please see the "Steps You Can Take to Protect Your Information" insert provided with this notice. This information provides additional steps you can take, including how to obtain a free copy of your credit report and place a fraud alert and/or credit freeze on your credit report.

For more Information

We understand that you may have questions about this incident that are not addressed in this letter. If you have questions, please call 1-866-775-4209, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

The JFC and <<ClientDef1(Entity Name)>> take the privacy and security of the personal information in our care seriously. We sincerely apologize for this incident and regret any concern or inconvenience this has caused you.

Sincerely,

Valerie Krueckeberg
Managing Director, Shared Business Services

Enclosure

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	freeze.transunion.com

Review of Account Statements Regularly. We recommend that you closely monitor your banking and credit account statements for suspicious activity on your existing accounts. You should remain vigilant by attentively monitoring your credit reports and account statements for indications of fraud and/or theft, including identity theft.

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. This notice has not been delayed as the result of a law enforcement investigation.

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

For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

Kroll.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.