



Randy V. Sabett
+1 202 728 7090
rsabett@cooley.com

VIA EMAIL

May 2, 2023

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

Re: Legal Notice of Information Security Incident

Dear Sir or Madam:

I write on behalf of our client, Kerecis LLC ("Kerecis"), to inform you of a security incident involving personal information for certain Kerecis employees. Kerecis will be providing notice to these individuals, including twenty Maryland residents, via written letter outlining some steps they may take to help protect themselves.

Kerecis recently became aware that some employees were identified by the IRS as potential victims of identity theft and Kerecis promptly launched an investigation. The investigation revealed that certain information of current and former employees may have been exposed on February 24, 2023. Kerecis determined that this was not a hack into their systems but likely the result of a sophisticated social engineering scheme.

Kerecis took steps to address this incident promptly after it was discovered including launching an investigation. Kerecis also promptly initiated its Incident Response Plan to determine what happened and has taken additional measures designed to help prevent this type of incident from reoccurring in the future such as implementing tighter security restrictions, upgrading email structures and notifications, and improving internal training on data security issues. These measures are in addition to those Kerecis regularly maintains, which include internal security audits and security training programs for all new hires and current employees. In addition, Kerecis has notified law enforcement and will assist them in their investigation.

As noted above, the affected individuals will be notified via written letter, which we expect will begin mailing on or around May 2nd, 2023. A form copy of the letter being sent to the potentially affected Maryland residents is included for your reference. If you have any questions or need further information regarding this incident, please contact me at +1 202 728 7090 or rsabett@cooley.com

Sincerely,

A handwritten signature in blue ink, appearing to read 'RS', is placed above the word 'Enclosure'.

Enclosure

2 1 355 *****SNGLP

SAMPLE A. SAMPLE - L02

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



May 2, 2023

NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to inform you of a security incident that involves certain of your personal information. While we have no evidence to suggest that your personal information has been misused, we are providing this notice to inform potentially affected individuals about the incident and to inform you of some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened?

On March 29, 2023, Kerecis became aware that some employees were identified by the IRS as potential victims of identity theft and the Company promptly launched an investigation.

What Information Was Involved?

The following elements of data may have been compromised:

- Full name
- Home address
- Social security number
- Salary amount
- Federal income tax amounts withheld
- State and local tax amounts withheld (where applicable)
- Name of local tax entity (where applicable)
- Medicare tax amounts withheld
- Employee social security tax amounts withheld

Our investigation has not found any evidence that this incident involves any unauthorized access to or use of any of our internal computer systems or network and based on our investigation, we believe the incident was a one-time occurrence. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

We take the privacy of personal information seriously and deeply regret that this incident occurred. We took steps to address this incident promptly after it was discovered including launching an investigation. We also promptly initiated our Incident Response Plan to determine what happened. We took steps to identify the data impacted and the source of the incident.

We have taken additional measures designed to help prevent this type of incident from reoccurring in the future such as implementing tighter security restrictions, upgrading email structures and notifications, and improving internal training on data security issues. These measures are in addition to those we have regularly maintained,

which include internal security audits and security training programs for all new hires and current employees. In addition, we have notified law enforcement and will assist them in their investigation.

To help protect your identity, we are offering two (2) years of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the enrollment instructions included with this letter.

What You Can Do

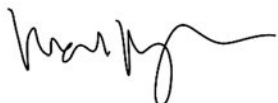
Although we are not aware of any widespread misuse of personal information, we are aware that fraudulent tax returns may have been submitted and we want to make you aware of steps that you can take as a precaution:

- **Activating the Complimentary Identity Protection Services.** We are offering two (2) years of identity theft protection and credit monitoring services at no charge to you. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the “Information about Identity Theft Protection” reference guide attached to this letter. Note that you must complete the enrollment process by July 31, 2023.
- **Checking Credit Reports and Financial Accounts.** You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff’s office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution immediately.
- **Report to Tax Agencies.** You can contact the IRS hotline at 800-908-4490 or visit <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft>. We are also providing an IRS Form 14039 “Identity Theft Affidavit” that can be filed with the IRS to help prevent someone from filing a fraudulent tax return in your name. There may also be similar resources and forms to file for individual states, so we recommend that you check directly with your state department of revenue for more information. Please note that a listing of state tax agencies’ websites is available at <http://www.taxadmin.org/state-tax-agencies>. The form can be found here: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>.
- **Reviewing Explanation of Benefits Documents.** You can also review explanation of benefits statements that you receive from your health insurer or health plan or review for persons whose medical bills you assist with or pay (such as your child). If you identify services listed on the explanation of benefits that were not received, please immediately contact your insurer or health plan.
- **Consulting the Identity Theft Protection Guide.** Finally, please review the “Information about Identity Theft Protection” reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact Nicol Dozier directly at 571-867-1412 between the hours of 9:00am -5:00pm Eastern time, Monday through Friday or via email at hr@kerecis.com. Again, we sincerely regret any concern this incident may cause.

Sincerely,



Mark A. Maghie, General Counsel

Information about Identity Theft Protection

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by July 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by July 31, 2023. Be prepared to provide engagement number **B089120** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For additional information from the IRS about identity theft, please visit <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft> or call 800-908-4490. There may be similar resources available at the state level, and you can contact your state department of revenue directly for more information. A listing of state tax agencies' websites is available at <http://www.taxadmin.org/state-tax-agencies>.

For District of Columbia Residents: You may obtain information about avoiding identity theft from the District of Columbia Attorney General's Office: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001, 202-727-3400, <https://oag.dc.gov/>.

For Iowa Residents: If you have been a victim of identity theft, you may also contact the Attorney General of Iowa at 1305 E. Walnut St., Des Moines, IA 50319, (515) 281-5164, www.state.ia.us/government/ag.

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. The mailing address for Kerecis is 2101 Wilson Boulevard, Suite 900, Arlington, VA 22201, and the general phone number is 703-287-8752.

For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/internet/privacy-and-identity-theft>.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

Security Freezes and Fraud Alerts: You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, 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.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity

before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports for no charge. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

By law, you also have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Additional Information for New Mexico Residents: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute incomplete or inaccurate information;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit "prescreened" offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a "security freeze" on your credit report.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and may need to provide the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity;

- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
- (4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For more information, including information about additional rights, you can visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>, <https://www.consumerfinance.gov/learnmore/>, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)	Experian (www.experian.com)	TransUnion (www.transunion.com)
General Contact:	General Contact:	General Contact, Fraud Alerts and Security Freezes:
P.O. Box 740241, Atlanta, GA 30374 800-685-1111	P.O. Box 2104, Allen, TX 75013 888-397-3742	P.O. Box 2000, Chester, PA 19022 800-916-8800
Fraud Alerts and Security Freezes:	Fraud Alerts and Security Freezes:	
P.O. Box 740256, Atlanta, GA 30374	P.O. Box 9556, Allen, TX 75013	