OUTSTATE TROWEL TRADES
FRINGE BENEFIT FUNDS

Michigan Trowel Trades Health & Welfare Fund
Outstate Michigan Trowel Trades Pension Fund
Michigan Operative Plasterers' & Cement Masons' International Association Apprenticeship and Training Fund

Managed for the Trustees by:
TIC INTERNATIONAL CORPORATION

October 10, 2022

Dear Participant,

On September 1, 2022, TIC International Corporation, the third party administrator for the Outstate Michigan Trowel Trades Pension Fund and the Michigan Trowel Trades Health and Welfare Fund, sent you a letter informing you of a recent incident in which TIC was the victim of a ransomware attack which resulted in the disclosure of certain participant's and beneficiary's personal information. We have enclosed a sample of that letter.

We are following up to make sure that you are aware of the incident, and that you know that TIC has offered to provide affected individuals with free credit monitoring services for 12 months if they enroll soon.

At this point, we are still working with TIC to confirm everyone who was supposed to receive a letter has received one. We can make presumptions about whose information may be at risk based on the description of the data that was acquired, but only TIC can tell us who was actually impacted because the breach occurred on TIC's systems. However, the Fund can confirm:

- The letter from TIC, see the enclosed sample, is not a scam request for your personal information;
- TIC is offering you credit monitoring services from Kroll, and;
- If you want to request Kroll's services, you must use the code from TIC and contact Kroll directly.

It is important that you take advantage of the free credit monitoring being offered if you were affected, but whether you were affected or not, you should take additional steps to protect yourself such as reviewing your account statements from financial institutions for suspicious activity, obtain and review copies of your credit report on a regular basis, and **consider placing a fraud alert or credit/security freeze on your credit report**.

We have enclosed more information regarding this matter in a question and answer format. This information may help you better understand what happened and how you might want to consider responding to these events.

Please contact Kroll at 855-544-2905 with any questions.

Sincerely,

Board of Trustees
Outstate Michigan Trowel Trades Pension Fund
Michigan Trowel Trades Health and Welfare Fund

6525 Centurion Drive • Lansing, MI 48917-9275
(517) 321-7502 • (877) 876-9357 Toll Free
FAX (517) 321-7508
www.outstatetroweltrades.org

TIC International Corporation
Benefit Administrators and Consultants
11590 North Meridian Street, Suite 600
Carmel, Indiana 46032-4529

<<b2b_text_4(MICHINGAN STATE PAINTERS INSURANCE FUND)>>

<<b2b_text_5(PAINTERS LOCAL UNION NO. 1052 PENSION TRUST FUND)>>

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (Re: Notice of Data Breach/ Data Incident)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to provide you with information about a recent data security incident that may have involved your personal information. TIC International Corporation ("TIC") administers health, pension, defined contribution/401(k), and other types of benefit funds. TIC is required to maintain records of your personal information because you are or have been a Participant of <<b2b_text_2 (Fund Names)>>. The purpose of this letter is to inform you about the incident, offer you identity monitoring services, and provide you with information, resources, and other steps you can take to help protect your personal information.

What Happened? On March 30, 2022, TIC experienced a system disruption due to an encryption attack. We hired cybersecurity experts to assist with our response and to determine whether any personal information was affected. The investigation determined that personal information was acquired during the incident. Following this confirmation, we underwent a thorough and extensive review of potentially affected files to determine what personal information may have been involved, locate mailing information, and set up the services being offered, which process was completed on August 22, 2022.

What Information Was Involved? The information involved included your <<b2b_text_3 ("name" and Data Elements)>>.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. We also reported the matter to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators accountable. We have also secured the services of Kroll to offer identity monitoring services at no cost to you for 12 months. 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 their confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (date)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do. You can follow the recommendations included with this letter to help protect your information. We encourage you to activate the free identity monitoring services.

For More Information: Further information about how to help protect your personal information is included with this letter. If you have questions or need assistance, please contact 855-544-2905, Monday through Friday, 8:00 am to 5:30 pm Central Time, excluding major U.S. holidays. Our representatives are fully versed on this incident and can answer any questions you may have.

We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

Ronald T. Fisher
Corporate Privacy and Security Officer

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—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 will be able to help you determine if it is 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.

$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.

$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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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.

Background and FAQs Related to TIC Data Incident

Participants and their family members may have recently received a notice on TIC letterhead regarding a data breach that recently occurred with TIC and offering 12 months of free credit/identity monitoring and protection from Kroll, a firm TIC hired with the help of its insurance carrier. **If you received the letter, you must act quickly to accept the free monitoring (generally before November 29, 2022 depending on the date the notice was mailed to you).**

This event is separate and distinct from other events that may have triggered similar notices to you in the past, such as the breach involving Wolverine or Morley Companies (both subcontractors to Blue Cross Blue Shield of Michigan).

What happened?

On March 30, 2022, TIC International Corporation, the third-party administrator for the Fund, was the victim of a ransomware attack perpetuated by "Conti", a Russian-affiliated criminal organization. The following summary is based on information provided by TIC.

Upon discovering the event, TIC took steps to secure its systems and launched an investigation with the assistance of a digital forensics firm provided by its insurance carrier. TIC also notified the FBI and its clients of the event. The initial notice to clients, sent on March 31, 2022, had to be sent via fax because the attack prevented TIC's use of e-mail.

TIC worked with a team of cybersecurity experts (including outside legal, forensic and remediation specialists) in order to respond to the attack. The attack essentially shut down TIC's operations when it first occurred, impacting e-mail and computer systems. TIC was able to restore those systems and its investigation, including a third party review of the potentially impacted data, was largely completed on August 22, 2022. The process of identifying the client funds to which some of the impacted records belong is ongoing (so new notices may continue to be issued until that process is fully completed).

TIC provided the Board its first written update on April 6, 2022. That update confirmed that most of TIC's data and services had been restored and that all April 1st benefit payments had been made on time.

TIC provided a second written update regarding the attack to the Board on April 29, 2022. For the first time, TIC reported that some participant data may have been accessible to, or possibly acquired by, the hackers. The update also identified a number of steps TIC had taken to improve its cybersecurity position and improve its abilities to avoid future attacks. TIC worked to improve and increase the training of its staff with respect to cybersecurity and implemented additional safeguards intended to better protect participant information, such as implementing enhanced access protocols, enhanced security configuration of perimeter devices, enhanced endpoint monitoring software (tools used to detect malicious behavior of bad actors who have gained or are attempting to gain unauthorized access to an entity's systems), and 24/7 live monitoring of TIC's systems by a security operations center.

Negotiators provided by TIC's insurance carrier took approximately a month to obtain confirmation of which files had been acquired by the hackers. They confirmed over 40,000 files were acquired.

The digital forensics firm used by TIC then sought to confirm whether and to what extent personal information (names, addresses, dates of birth, and Social Security numbers) was included in the acquired files.

TIC has reported the files acquired consisted primarily of archived tax records: Forms 1095, Forms 1099, and the data files TIC used to prepare those forms. The archived records included files dating as far back as the 1998 tax year. In addition, there was a subset of files in other directories (non-tax records) acquired by the hackers. These records have been described as scanned documents, such as divorce records and qualified domestic relations orders. Not all of the acquired files were specifically identified to an individual client, which required TIC and its providers to trace the record back to a specific fund client before it could confirm which clients and participants (current and former) had been impacted.

On July 26, 2022, TIC sent an update to the Board reporting that data had been accessed or acquired as a result of the incident. In that update, TIC provided a draft letter it planned to send to affected participants and beneficiaries.

Around September 1, 2022, TIC began sending notices to participants and beneficiaries impacted by the breach. TIC has offered to provide monitoring only to those whose Social Security numbers were included in the breach and is providing a dedicated telephone assistance line to answer participant questions. The line is run by Kroll.

There has been anecdotal information that the letters being sent only identify name and Social Security number as the data elements involved in the hack. However, the information acquired in the breach may have contained address and date of birth in addition to name and Social Security number. The Funds have followed up on our prior requests to TIC and are seeking answers to additional questions raised by this recent distribution of letters. We have not received a complete response at this time.

One of our concerns at the present time is that the notices may not accurately identify all of the data elements acquired in the breach. We are working with TIC to address this issue and will direct TIC to provide corrected notices, as needed.

What data was acquired?

TIC's investigators determined that approximately 40,000 files were accessed or acquired by the hackers. TIC has reported the files acquired consisted primarily of archived tax records: Forms 1095, Forms 1099, and the data files TIC used to prepare those forms. The archived records included files dating as far back as 1999. In addition, there was a subset of files in other directories (non-tax records) acquired by the hackers. These records have been described as scanned documents, largely divorce records and qualified domestic relations orders. Not all of the acquired files were specifically identified to an individual client, which required TIC and its providers to trace the record back to a specific fund client before it could confirm which clients had been impacted.

Form 1095-B is used to report certain information to the IRS and to taxpayers about individuals who are provided minimum essential health coverage by a health fund. That form has been prepared annually since 2016 (2015 tax year) and includes the participant's name, address, the last four digits of their Social Security number (or date of birth if the Social Security number is not available) and identifies other covered individuals (such as a spouse or children) along with the last four digits of their Social Security number (or date of birth if the Social Security number is not available). The Form also discloses the name, address, and phone number of your health insurance provider. TIC's data file used to create the Form 1095 includes the full Social Security number and date of birth for the participant. That file generally includes the Social Security number for dependents, but may not have the date of birth for all dependents.

Form 1099 is a series of forms the IRS refers to as "information returns." There are a number of different 1099 forms that report various types of benefit payments individuals may receive throughout the year, such as pension benefit payments reported on a 1099-R. Some medical and health care payments may be reported on Form 1099-

MISC. Forms 1099 are prepared annually and include the name of the person who received the payment (participant or beneficiary), their address, and Social Security number. Forms 1099 do not include the individual's date of birth.

I didn't receive a letter, does that mean my data is still safe? Or if my child or spouse received a letter but I did not, is my data still safe?

At this point, we are still working with TIC to confirm everyone who was supposed to receive a letter has received one. We can make presumptions about whose information may be at risk based on the description of the data that was acquired, but only TIC can tell us who was impacted because the breach occurred on TIC's systems. For example, based on the description of the data acquired, it is not clear how a dependent's data might have been acquired without the participant's data also being acquired. With the ever-increasing number of breaches in our society, it is best to be vigilant in monitoring your credit information—whether or not you have been impacted by this breach occurring with TIC. However, if your data was affected by this breach, TIC should arrange for you to receive a notice. Please make sure your contact information with TIC is current.

I received a letter; what should I do now?

We suggest you call Kroll at 855-544-2905 or visit the website https://enroll.krollmonitoring.com to sign up for the free credit monitoring being offered. As explained in the letter, while it is important that you take advantage of the free credit monitoring being offered, but you should also take additional steps such as reviewing your account statements from financial institutions for suspicious activity, obtain and review copies of your credit report on a regular basis, and consider placing a fraud alert or security freeze on your credit report.

My letter only says my Social Security number was acquired, not my date of birth. Is that a big deal?

It is not yet clear if letters reporting that only the name and Social Security number were acquired are accurate. The records acquired would likely have had name, Social Security number, date of birth and address. With your date of birth and Social Security number, a criminal can more easily steal your identity. It is important that you take advantage of the free credit monitoring being offered, but you should also take additional steps such as reviewing your account statements from financial institutions for suspicious activity, obtain and review copies of your credit report on a regular basis, and consider placing a fraud alert or credit/security freeze on your credit report.

If my personal information was accessed by an unauthorized party, does that mean that I will become a victim of identity theft?

Not necessarily. Even if someone did access your information, this does not mean that you have been, or will become, a victim of identity theft or that the unauthorized individual intends to use your personal information to commit fraud. TIC notified you about this incident so you can take steps to protect yourself. You can do this in several ways, including: by accepting the offer of free credit monitoring for 12 months; by placing a fraud alert on your credit file; by placing a credit/security freeze on your credit report; and by reviewing your credit reports and account statements regularly.

I no longer have the code because I threw the letter away. How do I get a new code?

If you call Kroll at 855-544-2905, you can identify yourself and they can provide you with the code if you are on the list of impacted individuals. If you were not on the list, you may still want to consider taking actions described above to protect your identity.

Why does Kroll need my Social Security number to provide monitoring services?

Your Social Security number is used for the identity verification process Kroll requires to create your account and start the monitoring services. During the sign-up process, Kroll uses your personal information, such as your Social Security number, to display identity verification questions to which the answers are unique to your background information.

What do I do if I am having trouble signing up with Kroll?

If you are experiencing issues signing up for your monitoring services online, first check that you are entering your information correctly, including membership number, last name, and zip code, as it is indicated in your letter. If you are still experiencing issues signing up, Kroll recommends you clear your browser history and any cached information, then try to sign up again.

If after following these steps you are still having difficulty, call Kroll at 855-544-2905 and explain difficulty you are experiencing. If Kroll is not helpful, you may contact TIC directly at 517-321-7502 and explain the difficulty you are experiencing.

How do I sign my kids up for credit monitoring when I only have one e-mail address and I already used it for myself?

If you do not want to create a new e-mail address for your child, many popular email providers allow users to create alias or disposable email addresses. These additional addresses can be used to sign up for services and are delivered to your inbox, just like your primary email address. If your email address is provided by Google/gmail, Apple/iCloud, or Microsoft Outlook, you can add "+something" before the @ symbol and it will still go to the same inbox. For example sending something to “yourname+something@email.com” would still be received in the inbox for “yourname@email.com” so long as the email provider supported this method for aliases. See, https://login.krollmonitoring.com/duplicate-email, for more information or visit your e-mail provider’s website.

I signed up for the free credit monitoring, should I do any of the other things suggested in the letter?

It is important that you take advantage of the free credit monitoring being offered, but you should also consider additional steps such as reviewing your account statements from financial institutions for suspicious activity, obtaining and reviewing copies of your credit report on a regular basis, and placing a fraud alert or credit/security freeze on your credit report.

Credit monitoring is helpful, but generally notifies you after the fact. These additional steps may be more important from a long term view point than the credit monitoring. Even after the credit monitoring has expired, you can continue to vigilantly review your account statements and credit report. You are entitled to receive a free credit report once a year from each of the three credit reporting agencies: Experian, Transunion and Equifax. You can also continue any credit/security freeze you put in place. A credit/security freeze can be preventative as new credit generally cannot be opened without a pin or password that you receive when initiating the freeze. However, a credit freeze is not completely fail-safe because creditors can issue credit without pulling a credit report. Also,

a credit freeze will not prevent current creditors and businesses with which you have prior relationships (such as credit card companies, insurance providers and financial institutions) from reporting to or accessing your credit information. It does, however, prevent new potential creditors and new third parties from gaining access to your credit information.

What is credit monitoring?

Credit monitoring services protect primarily against new account fraud. This form of fraud occurs when a criminal uses your personal information to open a credit card, mobile phone, or other financial accounts using your name, Social Security number and other personal information. New account fraud can be difficult to detect because the criminal generally has billing statements sent to an address other than your real address. Beginning on the date of enrollment, credit monitoring provides an alert whenever changes occur to your credit file with the credit bureau that is being monitored. This notification will be sent to you the same day that the change or update takes place with the credit bureau being monitored.

What is included with the free credit monitoring being offered?

In addition to 12 months of free single bureau credit monitoring, TIC's offer includes providing Web watcher (a service that watches for your personal information being sold on known criminal websites), $1 Million Identity Fraud Loss Reimbursement (a service that can reimburse you for out of pocket expenses tied to an identity theft event), Fraud Consultation (a service that provides consulting on how to effectively protect your identity), and Identity Theft Restoration (a service that can work with you to resolve issues if you become a victim of identity theft), all from Kroll. These services are described in the notice that was mailed by TIC and are subject to the terms of the policy Kroll issues. You can learn more about these services by calling Kroll at 855-544-2905.

What is a fraud alert?

Most credit card companies and other creditors will not issue credit without first checking an applicant's credit history. A fraud alert tells potential creditors that they should contact you first before issuing new credit in your name, thereby preventing someone from fraudulently obtaining credit without your knowledge. A fraud alert will not prevent you from using your credit cards or other accounts. A fraud alert, however, may slow the process of receiving new credit since the purpose of the fraud alert is to help protect you against an identity thief opening new credit accounts in your name. When you place a fraud alert on your account, potential creditors receive a message instructing them to re-verify the identity of the person applying for credit before approving the credit application. There is no charge for placing a fraud alert on your credit file. An initial fraud alert lasts for 90 days and is free. You may renew the fraud alert at no cost for an additional 90 days. There is no limit to the number of times you can renew the fraud alert.

How Do I put a fraud alert in place?

You can place a fraud alert on your credit file by contacting any one of the three national credit bureaus: Equifax (1-800-525-6285), TransUnion (1-800-916-8800) and Experian (1-888-397-3742). As soon as one credit bureau confirms your fraud alert, the others are also notified to place fraud alerts on your credit file.

What is a credit freeze or security freeze?

A credit freeze, also known as a security freeze, prohibits a credit bureau from releasing your credit report without your consent. However, placing a security freeze may delay, interfere with or prohibit the timely approval of any

application you then make regarding a new loan, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular telephone, utilities, digital signature, Internet credit card transaction or other services, including an extension of credit at a point of sale. Because of this, you may need to remove or temporarily lift the freeze. Also, if you have a security freeze in place and decide to apply for credit monitoring, you might need to temporarily lift the security freeze and then re-activate it after you are enrolled in credit monitoring. Depending where you reside, credit bureaus may sometimes charge a fee for placing, removing or temporarily lifting a credit freeze.

How do I put a credit freeze or security freeze in place?

If you want to put a freeze in place, you need to do it at each of the three major credit bureaus: Equifax (1-800-525-6285), TransUnion (1-800-916-8800) and Experian (1-888-397-3742). If you request a freeze, be sure to store the passwords you'll need to lift the freeze in a safe place.

Why was there a delay in notifying me about this incident?

TIC indicated that it acted first to protect files that may not have been accessed or acquired and get its systems back up and running. But it was equally important to verify whose personal information was included in the impacted files, and what elements of that information were included, before notifying you about the incident. TIC discovered the incident on March 30, 2022. Following the attack, TIC began conducting a thorough forensic investigation. Because of the complexity of the investigation, the broad scope of potentially affected data (as noted above), and the detailed analysis required, it took time to identify files that might have been exposed and link them to fund clients and their participants. Confirming or obtaining current contact information for affected individuals, preparing and mailing notification letters to fund clients and affected participants regarding this incident, and setting up a toll-free call center also required additional time.

Do I need to notify the IRS?

The IRS Taxpayer Guide to Identity Theft advises that if your tax records are not currently affected by identity theft, but you believe you may be at risk, you can contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. See additional information at http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

What should I do if I believe my personal information has been used fraudulently?

You should immediately: (1) report the crime to your local law enforcement agency, (2) contact any creditors involved, and (3) notify all three credit bureaus. You may also choose to put a credit freeze on your file if you have not already done so; please note that there may be a cost associated with this. The Federal Trade Commission also provides a website where you can report identity theft and get a recovery plan, available at: https://www.identitytheft.gov/#/.