



May 9, 2018

CPT ID: <<ID>>  
<EmployeeName>  
<Address1> <Address2>  
<City>, <State> <Zip>

Dear <FullName>:

CPT Group Inc. (“CPT”) understands the importance of protecting the information it maintains. Regrettably, we write to inform you of a recent incident that may have involved your personal information, which was provided to CPT in connection with the <<CaseName>> class action settlement. This notice explains the incident, measures we have taken, and some steps you can take in response.

CPT is a class action settlement administrator. We send settlement notices to class members, answer questions class members may have, and processes settlement payments. To accomplish this function, we are provided with necessary data about class members, including certain types of personal information. The underlying class action was dismissed and is no longer active.

On February 8, 2018, CPT learned through its ongoing forensics investigation of a phishing email incident that certain emails and attachments could have potentially been accessed by an unauthorized person. The investigation, conducted with the assistance of a computer forensics firm, determined that an unknown individual had access to a CPT employee’s email account from November 22, 2017 through December 8, 2017. While some of the attachments were encrypted and/or password protected spreadsheets, CPT could not rule out the possibility that the spreadsheet passwords may have also been available to the attacker. Although, to date, we do not know that any of your sensitive personal information was accessed without permission, we are providing you this notification out of an abundance of caution. The information that could have been accessed in the affected employee’s account includes former class member names, addresses, and Social Security numbers.

We are notifying you so that you can take appropriate steps to protect yourself and to offer you a complimentary one-year membership to Kroll Identity Monitoring. 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, Fraud Consultation, and Identity Theft Restoration. For more information on identity theft prevention and Kroll Identity Monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website.

Visit [my.idmonitoringservice.com](http://my.idmonitoringservice.com) to activate and take advantage of your identity monitoring services.

You have until **July 26, 2018** to activate your identity monitoring services.

Membership Number: <<MonitoringCode>>

We sincerely regret that this incident occurred. In addition to providing you notice of the incident, CPT has taken substantial steps to enhance its existing network and email security, including implementing multi-factor authentication, and is re-educating and training its employees to help prevent a similar incident from happening in the future.

If you have questions about this incident or the recommended next steps, please toll-free 1-833-219-9086 Monday through Friday between 8:00 am and 5:30 pm Pacific Time.

Sincerely,

Julie Green  
Senior V.P. of Operations





## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> 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 can help you determine if it's an indicator of identity theft.

### **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.

<sup>1</sup> 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.

## **MORE INFORMATION ON WAYS TO PROTECT YOURSELF**

Even if you decline to take advantage of this complimentary credit monitoring and identity theft prevention service, we remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

If you believe you are the victim of identity theft, or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps you can take to avoid identity theft, as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW  
Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

**Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

**Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)

**TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper

identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.