



Sian M. Schafle  
 Office: 267-930-4799  
 Fax: 267-930-4771  
 Email: sschafle@mullen.law

1275 Drummers Lane, Suite 302  
 Wayne, PA 19087

February 6, 2019

**INTENDED FOR ADDRESSEE(S) ONLY**

**VIA U.S. MAIL**

Attorney General Xavier Becerra  
 Office of the Attorney General  
 PO Box 944255  
 Sacramento, CA 94244-2550

**Re: Supplemental Notice of Data Event**

Dear Attorney General Becerra:

We continue to represent Pharmacy Times Office of Continuing Professional Education, LLC ("PTCE"), and are writing to supplement the notice of data event submitted to your office under cover of November 13, 2018, attached as *Exhibit A* for ease of reference. As previously mentioned, the investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice and the previous notice, PTCE does not waive any rights or defenses regarding the applicability of California law or personal jurisdiction.

As outlined in our November 13, 2018 correspondence, PTCE worked with third-party forensic investigators to determine the nature and scope of an event involving unauthorized access to a file containing PTCE data, and to confirm the identity of the clients whose personally identifiable information was contained in the data file. PTCE continues to research address information for a limited number of individuals whose information was contained within the relevant data file. PTCE recently confirmed the identities and address information for approximately nine hundred fifty-six (956) California residents who had personally identifiable information in the data file including: Name, Social Security number, username and password, email address, and/or security prompt and answer. On or around February 6, 2019, PTCE will begin providing written notice of this incident to these potentially affected individuals. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit B*.

Although to date the investigation has found no evidence of actual or attempted misuse of personal information as a result of this event, PTCE is providing the nine hundred fifty-six (956) California residents who will receive notice of this event access to one (1) year of complimentary credit and identity monitoring services and identity restoration services through Kroll. These individuals may also contact PTCE's dedicated call center with questions regarding these services or the event.

Since our November 13, 2018 notice to your office, PTCE continues to implement additional safeguards to protect the security of information in its system. While PTCE has not been contacted by law enforcement

Attorney General Xavier Becerra  
February 6, 2019  
Page 2

regarding the event, PTCE remains available and will assist in any criminal investigation commenced by law enforcement in this matter.

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4779.

Very truly yours,

A handwritten signature in black ink that reads "Sian M. Schafle". The signature is written in a cursive, flowing style.

Sian M. Schafle of  
MULLEN COUGHLIN LLC

SMS:emp  
Enclosure

# **EXHIBIT A**



# XAVIER BECERRA

## *Attorney General*

[Search](#)[Translate Website](#) | [Traducir Sitio Web](#)

# Submit Data Security Breach

[Home](#) / [Privacy](#) / [Submit Data Security Breach](#)

## **This submission is required by California Civil Code s. 1798.29(e); California Civil Code s. 1798.82(f)**

**Note: This form is only for use by businesses and state and local government agencies,** which are required to submit a sample notice if they experience a breach of personal information involving more than 500 California residents.

**If you are a consumer who wishes to file a complaint, please use our online complaint form.**

### SECTION 1 - ATTACH SECURITY BREACH NOTIFICATION SAMPLE

#### Sample of Notice

California Civil Code s. 1798.29(e) and s. 1798.82(f) provide that "A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code." A copy of this notification will be made available online.

Click browse button to select file and then click upload to attach the file.


11/26/2018

Submit Data Security Breach | State of California - Department of Justice - Office of the Attorney General

Add a new file

[Choose File](#) CA - Exhibit 1 Packet.pdf

Upload

 More information

## SECTION 2 - INFORMATION FOR LAW ENFORCEMENT PURPOSES

The information provided in SECTION 2 is for DOJ use.

Organization Name

Pharmacy Times Office of Continuing Professional Education ("PTCE")

Address

2 Clarke Drive, Suite 100

City

Cranbury

State

New Jersey ▼

Zip Code

08512

Date(s) of Breach (if known)

Date(s) of Breach (if known)

Date

2018-07-06

E.g., 2018-11-26

11/26/2018

Submit Data Security Breach | State of California - Department of Justice - Office of the Attorney General

Date(s) of Breach (if known)

I'm not a robot

reCAPTCHA  
Privacy - Terms

Add another Date

Date(s) of Discovery of Breach

Date(s) of Discovery of Breach

Date

2018-09-17

E.g., 2018-11-26

Add another Date

Date(s) Individual Notice Provided to Consumers

Date(s) Individual Notice Provided to Consumers

Date

2018-11-13

E.g., 2018-11-26

Add another Date

Was notification delayed because of a law enforcement investigation?

N/A

- No

Yes

11/26/2018

Submit Data Security Breach | State of California - Department of Justice - Office of the Attorney General

## Type of Personal Information Involved in the Breach

- ☐ Driver's License Number or California ID Card Number Information
- ☐ Financial Information (e.g. account number, credit or debit card numbers)
- ☐ Medical Information
- ☐ Health Insurance Information
- ☐ Other

## Brief Description of the Breach

See Exhibit 1.

## Report Type

- ☐ N/A
- ☐ Addendum to Previous Report
- ☒ Initial Breach Report

## Breach Affecting

- ☐ N/A
- ☐ Fewer Than 500 Individuals
- ☒ 500 or More Individuals

## Approximate Number of Individuals Affected by the Breach

128,211

## Approximate Number of Californians Affected by the Breach

21,786

## Type of Entity

- ☐ - None -
- ☐ BSO - Businesses - Other
- ☐ BSF - Businesses - Financial and Insurance Services
- ☐ BSR - Businesses - Retail or Merchant
- ☐ EDU - Educational Institutions

Is the organization a small business, according to the Small Business Administration? \*

11/26/2018

Submit Data Security Breach | State of California - Department of Justice - Office of the Attorney General

Yes

No

- Unsure

(See the Small Business Administration's standards for defining a "small business":  
[www.sba.gov/sites/default/files/files/Size\\_Standards\\_Table.pdf](http://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf).)

## Type of Breach

Unintended disclosure

Hacking or malware

Payment Card Fraud

Insider

Physical loss

Portable device

Stationary device

- ✓ Other

If Type of Breach is "Other" please describe the type of breach here

Data file security misconfiguration

## Location of Breached Information

Network Server ▼

If Location of Breached Information is "Other" please describe the location here

## Was Substitute Notice Given?

N/A

- No

Yes

## Was Media Notice Given?



11/26/2018

Submit Data Security Breach | State of California - Department of Justice - Office of the Attorney General

N/A

- No

Yes

Name of company contact whom the Attorney General may contact for further information

Sian Schafle

Telephone Number

267-930-4799

Email address

sschafle@mullen.law

Was a law enforcement agency notified regarding the breach?

N/A

- No

Yes

If Yes, name of law enforcement agency and contact name and number

Was a police report filed?

N/A

- No

Yes

If yes, police report number

Submit form

Submit

## **eCrime**

eCrime Unit

High Technology Theft Apprehension and Prosecution (HTTAP) Program

Investigations & Guidelines

File a Complaint

## **Data Security Breach ( SB24 )**

Data Security Breach Reporting

Submit Data Security Breach

Search Data Security Breaches

## **Related Information**

2016 Data Breach Report, pdf

Breach Help: Tips For Consumers

Cybersafety

Data Breach Statistics, pdf

eCrime

Identity Theft

Privacy

## **SB24 Administration**

All Submitted Data Security Breaches

Published Data Security Breaches

11/26/2018

Submit Data Security Breach | State of California - Department of Justice - Office of the Attorney General

Pending Review of Data Security Breaches

Rejected Data Security Breaches

## **Data Security Breach ( SB24 )**

Data Security Breach Reporting

Submit Data Security Breach

Search Data Security Breaches

## **Related Information**

Communication Service Providers Legal Process Information

Cybersafety

Data Security Breach Reporting

Internet Crime Complaint Center

Money Wiring Scams



**STATE OF CALIFORNIA DEPARTMENT OF JUSTICE  
OFFICE OF THE ATTORNEY GENERAL**

Search

**WHO WE ARE**

About AG Xavier Becerra

History of the Office

Organization of the Office

## **WHAT WE DO**

Public Safety

Opinions and Quo Warranto

Research

Children & Families

Civil Rights

Consumer Protection

Environment & Public Health

Tobacco Directory

Tobacco Grants

## **OPEN GOVERNMENT**

Ballot Initiatives

Conflicts of Interest

Criminal Justice Statistics

Meetings and Public Notices

OpenJustice Initiative

Public Records

Publications

Regulations

## **Memorial**

Agents Fallen in the Line of Duty

## **Vote**

Register to Vote

## **WHAT WE'RE WORKING ON**

21st Century Policing

Children's Rights

Consumer Protection and Economic Opportunity

Environmental Justice

Equality

Health Care

Immigration

11/26/2018

Submit Data Security Breach | State of California - Department of Justice - Office of the Attorney General

[OpenJustice](#)

## **MEDIA**

[Consumer Alerts](#)

[Press Releases](#)

[Media Library](#)

## **CAREERS**

[Getting a State Job](#)

[Examinations](#)

[Job Vacancies](#)

[Internships & Student Positions](#)

[Attorney General's Honors Program](#)

[Earl Warren Solicitor General Fellowship](#)

[Office of the Attorney General](#)

[Accessibility](#)

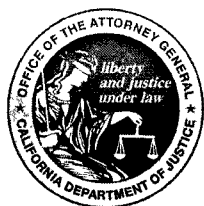
[Privacy Policy](#)

[Conditions of Use](#)

[Disclaimer](#)

© 2018 DOJ

State of California Department of Justice



**XAVIER BECERRA**  
*Attorney General*

Search

Translate Website | Traducir Sitio Web

# Data Breach Submission Confirmation

[Home](#) / [Privacy](#) / [Submit Data Security Breach](#) / [Data Breach Submission Confirmation](#)

Data Breach Report (SB24) *Submitted Breach Notification Sample* has been created. ✕

On behalf of the Office of the Attorney General, I would like to thank you for your submission.

## eCrime

eCrime Unit

High Technology Theft Apprehension and Prosecution (HTTAP) Program

Investigations & Guidelines

File a Complaint

## Data Security Breach ( SB24 )

11/26/2018

Data Breach Submission Confirmation | State of California - Department of Justice - Office of the Attorney General

Data Security Breach Reporting

Submit Data Security Breach

Search Data Security Breaches

## Related Information

2016 Data Breach Report, pdf

Breach Help: Tips For Consumers

Cybersafety

Data Breach Statistics, pdf

eCrime

Identity Theft

Privacy

## Related Information

Communication Service Providers Legal Process Information

Cybersafety

Data Security Breach Reporting

Internet Crime Complaint Center

Money Wiring Scams





**STATE OF CALIFORNIA DEPARTMENT OF JUSTICE  
OFFICE OF THE ATTORNEY GENERAL**

[Search](#)

**WHO WE ARE**

[About AG Xavier Becerra](#)

[History of the Office](#)

11/26/2018

Data Breach Submission Confirmation | State of California - Department of Justice - Office of the Attorney General

Organization of the Office

## **WHAT WE DO**

Public Safety

Opinions and Quo Warranto

Research

Children & Families

Civil Rights

Consumer Protection

Environment & Public Health

Tobacco Directory

Tobacco Grants

## **OPEN GOVERNMENT**

Ballot Initiatives

Conflicts of Interest

Criminal Justice Statistics

Meetings and Public Notices

OpenJustice Initiative

Public Records

Publications

Regulations

## **Memorial**

Agents Fallen in the Line of Duty

## **Vote**

Register to Vote

## **WHAT WE'RE WORKING ON**

21st Century Policing

Children's Rights

Consumer Protection and Economic Opportunity

Environmental Justice

Equality

Health Care

Immigration

11/26/2018

Data Breach Submission Confirmation | State of California - Department of Justice - Office of the Attorney General

[OpenJustice](#)

## **MEDIA**

[Consumer Alerts](#)

[Press Releases](#)

[Media Library](#)

## **CAREERS**

[Getting a State Job](#)

[Examinations](#)

[Job Vacancies](#)

[Internships & Student Positions](#)

[Attorney General's Honors Program](#)

[Earl Warren Solicitor General Fellowship](#)

[Office of the Attorney General](#)

[Accessibility](#)

[Privacy Policy](#)

[Conditions of Use](#)

[Disclaimer](#)

© 2018 DOJ

## Exhibit 1

We are writing to notify your office of an incident that may affect the security of personal information relating to twenty-one thousand seven hundred eighty-six (21,786) California residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PTCE does not waive any rights or defenses regarding the applicability of California law or personal jurisdiction.

**Nature of the Data Event**

On or about July 6, 2018, PTCE learned that an unauthorized party may have accessed a file containing PTCE data. PTCE immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the potential data event. Through this ongoing investigation, PTCE determined on September 17, 2018 that a file containing PTCE data had been publicly available between May 11, 2018 and July 6, 2018, and may have been subject to unauthorized access by an unknown party on or about July 6, 2018. On or around October 12, 2018, PTCE confirmed the file contained information including personally identifiable information for a limited number of PTCE clients. PTCE then took steps to confirm the identity of the clients whose personally identifiable information was contained in the data file.

PTCE began providing notice to the individuals potentially affected by this incident as soon as their address information was confirmed. The personal information impacted by this event may include the following: name, Social Security number, username and password, email address and/or security prompt and answer. To date, PTCE has not received any reports of the misuse of this information.

**Notice to California Residents**

On November 13, 2018, PTCE began providing written notice of this incident to affected individuals, which includes twenty-one thousand seven hundred eighty-six (21,786) California residents. Written notice was provided in substantially the same form as the letter attached here as *Exhibit A*.

**Other Steps Taken and To Be Taken**

Upon discovering the potential unauthorized access to the data file, PTCE moved quickly to identify those that may be affected, put in place resources to assist them, and provide them with notice of this incident. PTCE is also working to implement additional safeguards to protect the security of information in its system.

PTCE is providing written notice to those individuals who may be affected by this incident. This notice includes an offer of complimentary access to one (1) year of credit and identity monitoring services, including identity restoration services through Kroll, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, PTCE is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. PTCE is also providing written notice of this incident to other state regulators and the major consumer reporting agencies, as necessary.

## Exhibit A



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

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

Re: Notice of Data Breach

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

Pharmacy Times Office of Continuing Professional Education, LLC ("PTCE") is writing to inform you of a recent event that may impact the privacy of some of your personal information. We wanted to provide you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** On or about July 6, 2018, PTCE learned that an unauthorized party may have accessed a file containing PTCE data. PTCE immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the potential data event. On September 17, 2018, based on investigative developments to date, PTCE concluded that a file containing its data had been publicly available between May 11, 2018 and July 6, 2018, and on the latter date, may have been subject to unauthorized access by an unknown party. On or around October 12, 2018, PTCE confirmed that the file contained information that included personally identifiable information for a limited number of PTCE clients. PTCE then took steps to confirm the identity of the clients whose personally identifiable information was contained in the data file.

**What Information Was Involved?** The review of the file determined that the following types of your personal information was publicly accessible: **NAME, ADDRESS, PHONE NUMBER, EMAIL ADDRESS, CREDIT CARD INFORMATION**. To date, PTCE has not received any reports of the misuse of your information.

**What We Are Doing.** We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately removed the file from the web server. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state regulators, as required.

As an added precaution, we are also offering complimentary access to 12 months of identity monitoring, fraud consultation and identity theft restoration services through Kroll.

**What You Can Do.** You can find out more about how to protect against potential identity theft and fraud in the enclosed Steps You Can Take to Prevent Fraud and Identity Theft. There you will also find more information on the credit monitoring services we are offering and how to enroll.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-228-5723, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. Please have your Kroll membership number ready. This number can be found on the third page of this letter. You may also write to PTCE at 2 Clarke Drive, Suite 100 Cranbury, NJ 08512.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Jim Palatine, RPh, MBA  
 President

## Exhibit A

**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.

## Exhibit A

**STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION**

We have secured the services of Kroll to provide identity monitoring 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 confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **February 1, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-228-5723.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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](http://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.

You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

**Experian**  
PO Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-800-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

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

**TransUnion**  
P.O. Box 2000  
Chester, PA 19106  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

## Exhibit A

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit [www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more information.

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.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**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](http://www.ncdoj.gov).

**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](http://www.oag.state.md.us).

**For New Mexico residents**, 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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 [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.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.

**For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 804 Rhode Island residents impacted by this incident.



## Exhibit A



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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<ZipCode>>

## Re: Notice of Data Breach

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

Pharmacy Times Office of Continuing Professional Education, LLC ("PTCE") is writing to inform you of a recent event that may impact the privacy of some of your personal information. We wanted to provide you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** On or about July 6, 2018, PTCE learned that an unauthorized party may have accessed a file containing PTCE data. PTCE immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the potential data event. On September 17, 2018, based on investigative developments to date, PTCE concluded that a file containing its data had been publicly available between May 11, 2018 and July 6, 2018, and on the latter date, may have been subject to unauthorized access by an unknown party. On or around October 12, 2018, PTCE confirmed that the file contained information that included personally identifiable information for a limited number of PTCE clients. PTCE then took steps to confirm the identity of the clients whose personally identifiable information was contained in the data file.

**What Information Was Involved?** The review of the file determined that the following types of your personal information was publicly accessible: [PTCE Client Information](#). In addition to the foregoing, the following additional information may have also been publicly accessible: [PTCE Client Information](#). While this second set of information may not be considered protected data under applicable statutes, you are nonetheless being provided with notice out of an abundance of caution. To date, PTCE has not received any reports of the misuse of your information.

**What We Are Doing.** We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately removed the file from the web server. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state regulators, as required.

As an added precaution, we are also offering complimentary access to 12 months of identity monitoring, fraud consultation and identity theft restoration services through Kroll.

**What You Can Do.** You can find out more about how to protect against potential identity theft and fraud in the enclosed Steps You Can Take to Prevent Fraud and Identity Theft. There you will also find more information on the credit monitoring services we are offering and how to enroll.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-228-5723, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. Please have your Kroll membership number ready. This number can be found on the third page of this letter. You may also write to PTCE at 2 Clarke Drive, Suite 100 Cranbury, NJ 08512.

## Exhibit A

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,



Jim Palatine, RPh, MBA  
President



## 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.

## Exhibit A

**STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION**

We have secured the services of Kroll to provide identity monitoring 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 confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **February 1, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-228-5723.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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](http://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.

You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

**Experian**  
PO Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-800-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

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

**TransUnion**  
P.O. Box 2000  
Chester, PA 19106  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

## Exhibit A

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit [www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more information.

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.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**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](http://www.ncdoj.gov).

**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](http://www.oag.state.md.us).

**For New Mexico residents**, 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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 [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.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.

**For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 804 Rhode Island residents impacted by this incident.

## **EXHIBIT B**



Date: (Format: Month Day, Year)

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

**Re: Notice of Data Breach**

Dear <<MemberFirstName>> <<MemberLastName>>:

Pharmacy Times Office of Continuing Professional Education, LLC ("PTCE") is writing to inform you of a recent event that may impact the privacy of some of your personal information. We wanted to provide you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** On or about July 6, 2018, PTCE learned that an unauthorized party may have accessed a file containing PTCE data. PTCE immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the potential data event. On September 17, 2018, based on investigative developments to date, PTCE concluded that a file containing its data had been publicly available between May 11, 2018 and July 6, 2018, and on the latter date, may have been subject to unauthorized access by an unknown party. On or around October 12, 2018, PTCE confirmed that the file contained information that included personally identifiable information for a limited number of PTCE clients. PTCE then took steps to confirm the identity of the clients whose personally identifiable information was contained in the data file.

**What Information Was Involved?** The review of the file determined that the following types of your personal information was publicly accessible: (C) AND (D) FIRST AND LAST NAMES. To date, PTCE has not received any reports of the misuse of your information.

**What We Are Doing.** We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately removed the file from the web server. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state regulators, as required.

As an added precaution, we are also offering complimentary access to 12 months of identity monitoring, fraud consultation and identity theft restoration services through Kroll.

**What You Can Do.** You can find out more about how to protect against potential identity theft and fraud in the enclosed Steps You Can Take to Prevent Fraud and Identity Theft. There you will also find more information on the credit monitoring services we are offering and how to enroll.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-228-5723, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. Please have your Kroll membership number ready. This number can be found on the third page of this letter. You may also write to PTCE at 2 Clarke Drive, Suite 100 Cranbury, NJ 08512.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Jim Palatine, RPh, MBA  
 President



## 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.

## STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

We have secured the services of Kroll to provide identity monitoring 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 confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until May 7, 2019 to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-228-5723.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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](http://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.

You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

**Experian**  
PO Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

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

**TransUnion**  
P.O. Box 2000  
Chester, PA 19106  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)



Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit [www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more information.

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.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**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](http://www.ncdoj.gov).

**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](http://www.oag.state.md.us).

**For New Mexico residents**, 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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 [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.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.

**For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 840 Rhode Island residents impacted by this incident.



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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>

<<Address1>>

<<Address2>>

<<City>> <<State>> <<ZipCode>>

## Re: Notice of Data Breach

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

Pharmacy Times Office of Continuing Professional Education, LLC ("PTCE") is writing to inform you of a recent event that may impact the privacy of some of your personal information. We wanted to provide you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** On or about July 6, 2018, PTCE learned that an unauthorized party may have accessed a file containing PTCE data. PTCE immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the potential data event. On September 17, 2018, based on investigative developments to date, PTCE concluded that a file containing its data had been publicly available between May 11, 2018 and July 6, 2018, and on the latter date, may have been subject to unauthorized access by an unknown party. On or around October 12, 2018, PTCE confirmed that the file contained information that included personally identifiable information for a limited number of PTCE clients. PTCE then took steps to confirm the identity of the clients whose personally identifiable information was contained in the data file.

**What Information Was Involved?** The review of the file determined that the following types of your personal information was publicly accessible: **NAME, ADDRESS, PHONE NUMBER, EMAIL ADDRESS**. In addition to the foregoing, the following additional information may have also been publicly accessible: **DATE OF BIRTH, SOCIAL SECURITY NUMBER, CREDIT CARD NUMBER**. While this second set of information may not be considered protected data under applicable statutes, you are nonetheless being provided with notice out of an abundance of caution. To date, PTCE has not received any reports of the misuse of your information.

**What We Are Doing.** We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately removed the file from the web server. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state regulators, as required.

As an added precaution, we are also offering complimentary access to 12 months of identity monitoring, fraud consultation and identity theft restoration services through Kroll.

**What You Can Do.** You can find out more about how to protect against potential identity theft and fraud in the enclosed Steps You Can Take to Prevent Fraud and Identity Theft. There you will also find more information on the credit monitoring services we are offering and how to enroll.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-228-5723, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. Please have your Kroll membership number ready. This number can be found on the third page of this letter. You may also write to PTCE at 2 Clarke Drive, Suite 100 Cranbury, NJ 08512.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,



Jim Palatine, RPh, MBA  
President



## 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.

## STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

We have secured the services of Kroll to provide identity monitoring 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 confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until May 7, 2019 to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-228-5723.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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](http://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.

You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

**Experian**  
PO Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

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

**TransUnion**  
P.O. Box 2000  
Chester, PA 19106  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

- Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit [www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more information.

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.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**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](http://www.ncdoj.gov).

**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](http://www.oag.state.md.us).

**For New Mexico residents**, 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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 [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.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.

**For Rhode Island Residents**: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 840 Rhode Island residents impacted by this incident.