

# **EXHIBIT 1**

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PCS does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

### **Nature of the Data Event**

On November 18, 2021, PCS discovered suspicious activity related to an employee's email account. PCS promptly commenced an investigation to determine the nature and scope of the activity. The investigation determined that an unauthorized user was able to gain access to one email account between November 4 and November 18, 2021. PCS has also been working with and notified the FBI immediately. PCS completed a thorough review to determine whether sensitive information was present in the impacted files and folders. Upon receiving the initial results of the review, PCS worked diligently and retained a third-party to locate address information for the affected individuals and completed that effort on April 25, 2022.

The information that could have been subject to unauthorized access includes name, Social Security number and Driver's License or State ID number.

### **Notice to Maine Residents**

On May 25, 2022, PCS began providing written notice of this incident to impacted individuals. On or about May 27, 2022, PCS proceeded to provide written notice of this incident to nineteen (19) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, PCS moved quickly to investigate and respond to the incident, assess the security of PCS systems, and identify potentially affected individuals. Further, PCS notified federal law enforcement regarding the event. PCS is providing access to free credit monitoring services to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, PCS is providing impacted individuals with guidance on how to better protect against identity theft and fraud. PCS is providing individuals with 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.

PCS is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

# **EXHIBIT A**



Let our independence ignite yours.™

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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

<<b2b\_text\_2(NOTICE OF [SECURITY INCIDENT] / [DATA BREACH] - CA residents)>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>:

Private Client Services, LLC (“PCS”) is writing to notify you of a recent event that may affect the security of some of your information. This notice provides you with information about the event, our response, and steps you may take to better protect your information, should you feel it is appropriate to do so.

### What Happened?

On November 18, 2021, PCS discovered suspicious activity related to an employee’s email account. PCS promptly commenced an investigation to determine the nature and scope of the activity. The investigation determined that an unauthorized user was able to gain access to one email account between November 4 and November 18, 2021; and PCS has also been working with and notified the FBI immediately. We engaged in a comprehensive review of the full contents of the affected accounts to determine what, if any, sensitive information was contained within them. This review was completed on April 25, 2022 and identified that the affected email accounts contained certain information related to you. While we cannot be certain whether your information was actually viewed or acquired, we are unable to rule out such activity, and are therefore notifying you in an abundance of caution.

### What Information Was Involved?

We cannot confirm if the unauthorized person (s) accessed or viewed any specific information relating to you. However, we determined that the information present in the relevant account included your <<b2b\_text\_1(name, data elements)>>.

### What We Are Doing.

The security of information on our systems is one of our highest priorities, and PCS has strict security measures in place to protect the information in our care. Following discovery of this incident, we took immediate steps to further secure our environment and are in the process of implementing additional security measures. We are also offering complimentary identity monitoring services for 12 months through Kroll at no cost to you. 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. Information and instructions on how to activate these complimentary services can be found in the “Steps You Can Take to Help Protect Your Information” attached to this letter.

### What You Can Do.

While PCS has no evidence of any actual or attempted misuse of your information related to this incident, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) months. You may also activate to receive the complimentary identity monitoring services we are making available to you. Further information is enclosed in the “Steps You Can Take To Help Protect Personal Information” insert.

**For More Information.**

We understand that you may have questions that are not addressed in this letter. If you have additional questions or concerns, please call our dedicated assistance line at (855) 788-2618 which is available Monday through Friday 9:00 am – 6:30 pm CT.(Excluding Major US Holidays) You may also write Private Client Services, LLC at 2225 Lexington Road, Louisville, KY 40206.

Sincerely,

A handwritten signature in black ink, appearing to read 'Tim Graham', with a horizontal line extending to the left.

Tim Graham  
Chief Operations Officer  
Private Client Services, LLC

## STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

### Activate Identity Monitoring Services



#### 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.

##### **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.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, 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(activation deadline)>>* 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](http://info.krollmonitoring.com).

Additional information describing your services is included with this letter.

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.

##### **Monitor Your Accounts**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. 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 directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

### **Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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); and 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 District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and [oag@dc.gov](mailto:oag@dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [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 bureaus 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 New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 44 Rhode Island residents impacted by this incident.