PAUL HASTINGS

1(312) 499-6059
davidcoogan@paulhastings.com

January 12, 2024

Via E-Mail

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notice of Security Incident

To Whom It May Concern:

We represent ProFund Advisors LLC, ProFunds Distributors, Inc., and ProShare Services LLC (collectively, "ProShares") located at 7272 Wisconsin Avenue, 21st Floor, Bethesda, MD 20814. We write to notify you of a security event at Paycor HCM, Inc. ("Paycor"), a payroll service provider, which affected the security of certain personal information relating to approximately 80 Maryland residents. By providing this notice, ProShares does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data breach notification statute, or personal jurisdiction.

Nature of Security Event

Although ProShares no longer uses Paycor as its payroll vendor, Paycor notified ProShares on August 3, 2023 about a third-party software event that potentially affected the security of certain personal information relating to ProShares' current and former employees. Upon learning of the incident, ProShares launched an investigation and attempted to learn more about the incident from Paycor. Paycor reported that it used MOVEit Transfer software in the regular course of its business operations to securely transfer files. On or around May 31, 2023, Progress Software, the provider of the MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third-party. The third-party accessed ProShares' payroll data using the MOVEit Transfer software. Paycor undertook an investigation to determine what personal information was impacted by the MOVEit Transfer software vulnerability.

Notice to Maryland Residents

In August 2023, Paycor reported to ProShares that its investigation would be completed at the end of October. When ProShares did not receive confirmation in October from Paycor about the results of the investigation, ProShares elected to provide notice to its current and former employees about the possibility that their personal information was impacted and offered complimentary credit monitoring services. A copy of this written notice dated October 24, 2023 is attached to this letter.

On November 30, 2023, Paycor notified ProShares that it had completed its investigation and identified 164 current and former employees of ProShares whose information was affected, including approximately 80 Maryland residents. On December 8, ProShares provided a second notice to its current and former employees that confirmed their information was affected and offered complimentary credit

PAUL
HASTINGS

monitoring. The recipients of this notice largely overlapped with the recipients of the notice dated October 24, 2023. A copy of the written notice dated December 8, 2023 is attached to this letter.

Should you have any questions regarding this notification or other aspects of this data security event, please do not hesitate to contact us.

Sincerely,

/s/ David Coogan
for PAUL HASTINGS LLP

Enclosures

ProFunds

4145 SW Watson Ave.
Suite 400
Beaverton, OR 97005

ProFund Advisors LLC

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

October 24, 2023

Notice of Potential Data Breach

Dear <<First Name>> <<Last Name>>,

Paycor HCM, Inc. ("Paycor") provides payroll and related services for companies and other organizations, including ProFund Advisors LLC ("ProFunds"). Although Paycor is no longer our payroll vendor, Paycor recently notified us of a third-party software event that may affect the security of some of your information. While we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? Paycor utilizes MOVEit Transfer software in the regular course of its business operations to securely transfer files. On or around May 31, 2023, Progress Software, the provider of the MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. Paycor notified us of the incident and promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on their systems. Through the investigation, they learned that the third-party may have accessed ProFunds' payroll data using the MOVEit Transfer software. Paycor's investigation is ongoing and they have not yet confirmed the specific ProFunds' files that were impacted, if any.

Once we were contacted by Paycor and notified of the potential data exposure, we conducted a review of our records to confirm the identities of individuals potentially affected by this event. We are providing this notification to all potentially impacted individuals.

What Information Was Involved? Our review determined that the following types of information were in Paycor's system at the time of the event: name, Social Security number, bank account number, and date of birth. At this time, it has not been confirmed that any of this information has been breached.

What We Are Doing. We take this event and the security of information in our care very seriously. Upon learning about this vulnerability, we promptly took steps to require further investigation by Paycor and assess the security of your information both internally and at third-party vendors such as Paycor. In response to this event, we are also reviewing our information security policies and procedures for potential enhancements.

As an additional precaution, ProFunds is offering employees who may have been impacted identity theft protection services through IDX, a leading data breach and recovery services expert. The services offered by IDX include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and ID theft recovery services.

What You Can Do. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-800-939-4170, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time. Please note the deadline to enroll is January 24, 2024.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

*   *   *   *   *

In closing, ProFunds takes this event and the security of information in our care very seriously. We continue to investigate this matter and will keep you informed of any significant developments.

Sincerely,

Keith Gorman

Chief Human Resources Officer
(Enclosure)

IDX
A ZEROFOX COMPANY

Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia Residents: The District of Columbia Attorney General, 400 6th Street, NW, Washington, D.C. 20001; oag.dc.gov; Telephone: 1-202-727-3400.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

ProFunds

ProFund Advisors LLC

4145 SW Watson Ave.
Suite 400
Beaverton, OR 97005

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

December 8, 2023

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

Paycor HCM, Inc. ("Paycor") provides payroll and related services for companies and other organizations, including ProFund Advisors LLC, and its affiliates (collectively, “ProShares”). Although Paycor is no longer our payroll vendor, Paycor recently notified us of a third-party software event that affected the security of some of your information. We are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? Paycor utilizes MOVEit Transfer software in the regular course of its business operations to securely transfer files. On or around May 31, 2023, Progress Software, the provider of the MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third-party. The third-party accessed ProShares’ payroll data using the MOVEit Transfer software. Paycor recently concluded an extensive analysis and determined that some of ProShares’ employee data was affected as a result of this incident.

What Information Was Involved? Paycor’s investigation determined that the information that was breached was your name and Social Security number.

What We Are Doing. We take this event and the security of information in our care very seriously. In response to this event, we are also reviewing our information security policies and procedures for potential enhancements.

In addition, ProShares is offering employees who were impacted identity theft protection services through IDX, a leading data breach and recovery services expert. The services offered by IDX include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and ID theft recovery services.

What You Can Do. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-800-939-4170, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time. Please note the deadline to enroll is January 24, 2024.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

In closing, ProShares takes this event and the security of information in our care very seriously. We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Sincerely,

Keith Gorman

Chief Human Resources Officer
(Enclosure)

A ZEROFOX COMPANY

Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia Residents: The District of Columbia Attorney General, 400 6th Street, NW, Washington, D.C. 20001; oag.dc.gov; Telephone: 1-202-727-3400.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.