



Matthew Toldero, Esq.
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
One West 4th Street, Suite 850
Winston-Salem, NC 27101
mtoldero@constangy.com
336.448.8552

July 15, 2024

VIA ELECTRONIC MAIL

Attorney General Brown
Office of the Attorney General
Department of Professional and Financial Regulation
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Insight Meditation Society, Inc. ("IMS"), located in the State of Massachusetts, in connection with the recent data security incident described below. Please be advised IMS reserves all rights, claims and defenses in connection herewith.

On March 23, 2024, IMS discovered an instance of IMS data published on the Internet. In response, IMS initiated an investigation to determine the full nature and scope of the issue. The investigation determined an unauthorized individual downloaded one (1) file from the IMS web server, which file contained some applicant information, but did NOT contain any payment information. IMS confirmed no computers, servers or other systems were potentially at risk.

With the assistance of a data review team, we conducted a thorough review of the affected data. This review was completed on May 30, 2024 and it was determined that personal information was present. IMS then needed to complete an extensive review to confirm identities and identify address information to provide notification. That effort was completed on June 13, 2024, it was then that IMS determined that the incident may have affected personal information belonging to Maryland residents. The affected information may have included individuals' names, medical or health care information, and medical history. June 15, 2024, IMS provided notice of this incident to approximately forty-two (42) Maryland residents via U.S. Mail. A sample copy of the notification letter is included with this correspondence as ***Exhibit A***.

In providing notice, IMS is also providing individuals with steps to take to help protect information, as well as the ability to reach out to a call center, if needed.

Should you have any questions or require additional information, please do not hesitate to contact me at mtoldero@constangy.com.

Sincerely,

A handwritten signature in black ink that reads "Matthew Toldero". The signature is written in a cursive, flowing style.

Matthew Toldero, Esq.

Alabama Arkansas California Colorado District of Columbia Florida Georgia Illinois
Indiana Maryland Massachusetts Minnesota Missouri New Jersey New York
North Carolina Oregon Pennsylvania South Carolina Tennessee Texas Virginia Washington

EXHIBIT A



P.O. Box 989728
West Sacramento, CA 95798-9728

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

<<Date>>

<<Variable Text >>

Dear << First Name>> << Last Name>>:

Insight Meditation Society, Inc. ("IMS") is writing to notify you of a recent incident that may have affected your personal information. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information.

What Happened? On March 23, 2024, IMS discovered an instance of IMS data published on the Internet. In response, IMS initiated an investigation to determine the full nature and scope of the issue. The investigation determined an unauthorized individual downloaded one (1) file from the IMS web server, which file contained some applicant information, but did NOT contain any payment information. IMS confirmed no computers, servers or other systems were potentially at risk.

With the assistance of a data review team, we conducted a thorough review of the affected data. This review was completed on May 30, 2024 and it was determined that personal information was present. IMS then needed to complete an extensive review to confirm identities and identify address information to provide notification. That effort was completed on June 13, 2024. Please note that IMS has no evidence of the misuse or attempted misuse of any potentially affected information.

What Information was Involved? The information that may have been affected in connection with this incident includes your name as well as your <<Variable Text 2>>. Again, please be assured no payment card information was potentially impacted.

What Are We Doing? As soon as we discovered the incident, we took the steps discussed above, and we have worked with our web developer to remedy the issue involving the web server.

What You Can Do. We recommend that you review the *Steps You Can Take to Help Protect Your Information* included with this letter for guidance on how you can protect your information.

For More Information: If you have questions about this letter or need assistance, please call do not hesitate to contact IDX at 1-800-939-4170 IDX representatives are available Monday through Friday from 6:00AM -6:00PM Pacific Time.

We take your trust in us very seriously and thank you for your understanding in this matter.

Sincerely,

Insight Meditation Society

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords.

If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report and obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is listed below:

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

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

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active-Duty Military Fraud Alert on their credit reports while deployed. An Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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

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

EXHIBIT A



P.O. Box 989728
West Sacramento, CA 95798-9728

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

<<Date>>

<<Variable Text >>

Dear << First Name>> << Last Name>>:

Insight Meditation Society, Inc. ("IMS") is writing to notify you of a recent incident that may have affected your personal information. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information.

What Happened? On March 23, 2024, IMS discovered an instance of IMS data published on the Internet. In response, IMS initiated an investigation to determine the full nature and scope of the issue. The investigation determined an unauthorized individual downloaded one (1) file from the IMS web server, which file contained some applicant information, but did NOT contain any payment information. IMS confirmed no computers, servers or other systems were potentially at risk.

With the assistance of a data review team, we conducted a thorough review of the affected data. This review was completed on May 30, 2024 and it was determined that personal information was present. IMS then needed to complete an extensive review to confirm identities and identify address information to provide notification. That effort was completed on June 13, 2024. Please note that IMS has no evidence of the misuse or attempted misuse of any potentially affected information.

What Information was Involved? The information that may have been affected in connection with this incident includes your name as well as your <<Variable Text 2>>. Again, please be assured no payment card information was potentially impacted.

What Are We Doing? As soon as we discovered the incident, we took the steps discussed above, and we have worked with our web developer to remedy the issue involving the web server.

What You Can Do. We recommend that you review the *Steps You Can Take to Help Protect Your Information* included with this letter for guidance on how you can protect your information.

For More Information: If you have questions about this letter or need assistance, please call do not hesitate to contact IDX at 1-800-939-4170 IDX representatives are available Monday through Friday from 6:00AM -6:00PM Pacific Time.

We take your trust in us very seriously and thank you for your understanding in this matter.

Sincerely,

Insight Meditation Society

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords.

If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report and obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is listed below:

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

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

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active-Duty Military Fraud Alert on their credit reports while deployed. An Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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

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