INSIGHT PARTNERS

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

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<last_name>>,

As you are likely already aware, Insight Partners experienced a personal data security breach earlier this year. We are writing today to formally notify you that your personal data was affected by this breach, and provide information to assist you in mitigating potential risks.

We take this incident seriously and sincerely regret any inconvenience it may have caused.

WHAT HAPPENED?

On January 16, 2025, Insight Partners' information technology ("IT") team detected that an unauthorized third-party had gained access to information systems used by the Insight Partners human resources and finance teams.

Insight Partners' investigation into the incident determined that, on or around October 25, 2024, a threat actor successfully used a sophisticated social engineering attack to gain access to the affected servers. Once inside, the threat actor began exfiltrating data from these servers, and beginning at or around 10:00 a.m. EST on January 16, 2025, began encrypting these servers.

Working with third party investigators and cybersecurity experts, Insight Partners took immediate efforts to contain and remediate the incident, and to expel the threat actor from Insight Partners' systems, which it successfully did on January 16, 2025.

WHAT INFORMATION WAS INVOLVED?

The investigation confirmed that your personal data was affected by this incident, including the following types of personal data:

<<b2b_text_1 (data elements)>><<b2b_text_2 (data elements cont.)>>.

Given the types of personal data affected by this breach, there is some risk that such data may be used by malicious actors for fraudulent purposes, such as identity theft. However, to date, we have no evidence to suggest that your personal data has in fact been misused in any way.

WHAT WE ARE DOING

Insight Partners has implemented necessary security measures to re-secure affected systems and to prevent similar occurrences in the future. For instance, Insight has addressed the misconfiguration that allowed the threat actor to

gain access; rebuilt compromised machines and all affected servers; and strengthened internal security and system access requirements. Insight has also notified law enforcement and regulatory authorities in relevant jurisdictions.

As a precaution, we are also offering you a complimentary <<Monitoring Term Length (Months)>> month [Equifax WebDefend membership] at no cost to you. Please find details on signing up for your [WebDefend] membership and additional information describing these services at the end of this letter.

WHAT YOU CAN DO

As noted above, Insight Partners has no evidence that your personal data has, in fact, been misused. As a best practice, you should remain vigilant and carefully review your personal and work accounts for any suspicious activity. Insight Partners also urges you to consider the following actions to protect your personal data:

- Activate the complimentary identity theft protection services by following the instructions in this letter.
- Change personal and enterprise passwords, and ensure that two-factor authentication is enabled on all financial accounts. If you detect any unauthorized activity on an account, you should change the password and security questions associated with the account.
- Monitor your credit information, and initiate a fraud alert with all three credit bureaus, and considering placing a freeze on your credit reports.

FOR MORE INFORMATION

If you have questions, please call [U.S. call center number], Monday through Friday from [9:00 a.m. to 5:00 p.m., EST].

We sincerely regret any inconvenience that this matter may have caused you.

Best Regards,

Andrew Prodromos

Managing Director & Chief Compliance Officer

INSIGHT PARTNERS

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

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

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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	**Experian**:	**TransUnion**:
equifax.com equifax.com/personal/credit-report-services P.O. Box 740241 Atlanta, GA 30374 866-349-5191	experian.com experian.com/help P.O. Box 2002 Allen, TX 75013 888-397-3742	transunion.com transunion.com/credit-help P.O. Box 1000 Chester, PA 19016 888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays 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.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 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 violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado, Delaware, and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Georgia, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, http://www.ag.ny.gov/home.html, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, http://www.dos.ny.gov/consumerprotection, 1-800-697-1220.

For Rhode Island residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes. You may also contact the Rhode Island Office of the Attorney General, 150 South Main Street Providence, Rhode Island 02903, http://www.riag.ri.gov, (401) 274-4400.