DESKNET
Smart Customer Engagement

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

<<date>>

Subject: Notice of Data <<Variable Text 1: Breach or Security Event>>

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

DeskNet, Inc. ("DeskNet") writes to inform you of a recent data security event that may have affected your personal information. At DeskNet, 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 event and steps that you can take to help protect your personal information.

What Happened? On or about September 2, 2025, we experienced an IT outage that disrupted access to certain local systems. After detecting and promptly containing the incident, we launched an investigation with the support of external cybersecurity experts to learn more about the scope of the incident and any impact to data. Through that investigation, we learned of information suggesting that an unknown actor gained unauthorized access to our network between August 31, 2025 and September 2, 2025 and potentially acquired certain files, some of which may have contained personal information. On or about December 4, 2025, DeskNet learned that your personal information may have been involved in connection with the incident which is the reason for this notification.

What Information Was Involved. We reviewed the accessible files and identified your name along with your Social Security number.

What We Are Doing. As soon as we discovered this incident, we launched an investigation and took steps to secure our IT environment, including implementing enhanced security measures to help prevent a similar incident from occurring in the future. DeskNet also notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrator(s) of the incident accountable.

In addition to providing resources you can utilize to help protect your information, DeskNet is also providing you with the opportunity to enroll in complimentary credit monitoring and identity theft protection services through CyberScout, a TransUnion company ("CyberScout") specializing in fraud assistance and remediation services. The complimentary credit monitoring and identity theft protection and resolution services include: a $1,000,000 identity theft insurance policy, at no charge to you. CyberScout's services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. These services also include proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. Please note, the deadline to enroll is **<<Deadline>>**.

To enroll in these services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: <<**UNIQUE CODE**>>. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do. We encourage you to enroll in the complimentary credit protection services we are offering. With this protection, Equifax can help you resolve issues if your identity is compromised. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information. If you have any questions regarding this event or need assistance, please call Mike Fitzsimons at DeskNet at 201-846-7080 x1005 between 9:00am to 5:00pm Eastern Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

DeskNet, Inc.
30 Montgomery St., Ste. 650
Jersey City, NJ, 07302-3835

Steps You Can Take to Help Protect Your Personal 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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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 (the "FTC").

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 www.annualcreditreport.com/, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 105851	P.O. Box 9532	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-833-799-5355
www.equifax.com	www.experian.com	www.transunion.com/get-credit·

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. 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 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. 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. For TransUnion: www.transunion.com/credit-freeze.

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.

Federal Trade Commission	New York Attorney General	NY Bureau of Internet and Technology
600 Pennsylvania Ave, NW	The Capitol	28 Liberty Street
Washington, DC 20580	Albany, NY 12224	New York, NY 10005
https://consumer.ftc.gov	https://ag.ny.gov	www.dos.ny.gov/consumerprotection/
877-438-4338	800-771-7755	212-416-8433

You also have certain rights under the Fair Credit Reporting Act ("FCRA"): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.