

[DATE]

NOTICE OF DATA BREACH

Dear [INDIVIDUAL NAME],

At Community Phone, we believe that the privacy and security of your information is of utmost importance, which is why we are writing to let you know about a data security incident that may involve your personal information.

WHAT HAPPENED?

On July 2, 2025, we became aware that some of our customers had received phishing emails, purportedly from Community Phone. We immediately began an investigation and took steps to limit the phishing emails' success. As a result of our investigation, on July 9, 2025, we discovered that on July 2, 2025, an unauthorized person had gained access to a Community Phone contractor's account on a third-party platform that Community Phone uses to record its sales and customer service calls. We immediately secured that account and began working with the third-party platform to determine what information may have been accessed.

WHAT INFORMATION WAS INVOLVED?

The unauthorized person may have accessed transcripts of Community Phone's sales and customer service call recordings, which may include your name, email address, your method of payment (credit card number, credit card expiration date, credit card verification number, bank account number, bank account routing number), and the fact that you have unlimited minutes in your phone plan.

WHAT WE ARE DOING

We took immediate action to investigate and remediate this incident. We provided notification to the potentially affected individuals as quickly as possible; this notice was not delayed because of a law enforcement investigation. We have implemented additional security measures designed to prevent the recurrence of such an incident and to protect the privacy of our valued customers. We will continue to review our existing policies and procedures and to assess options to further protect your information.

WHAT YOU CAN DO

Watch out for suspicious emails. Community Phone will never ask for your payment information using Google Forms. You should not provide personal information in response to any email regarding data security incidents. In addition, please review the attachment to this letter (Steps You Can Take to Protect Your Personal Information). This attachment describes further steps you can take to help protect your personal information, including monitoring your accounts and credit reports for any unauthorized activity and placing a fraud alert or credit freeze on your credit file.

FOR MORE INFORMATION

You can give us a call at 833-779-2921 between 8 a.m. and 10 p.m. ET Monday through Friday and 10 a.m. to 7 p.m. ET Saturday and Sunday. You can also write to us at 867 Boylston Street, 5th Floor #1503, Boston, MA 02116.

Sincerely,

Community Phone

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Monitor Your Accounts and Credit Report. We recommend that you regularly review your account statements and periodically obtain your credit report from one of the three major credit reporting agencies to monitor for unauthorized activity, including activity that may be a result of fraud or identity theft. You can 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 Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the printable request form at <https://www.annualcreditreport.com/manualRequestForm.action>. You can also purchase a copy of your credit report by contacting one or more of the three major credit reporting agencies listed below:

Equifax 1-800-685-1111 equifax.com/personal/credit-report-services <i>Credit report:</i> P.O. Box 740241 Atlanta, GA 30374-0241 <i>Credit freeze:</i> P.O. Box 105788 Atlanta, GA 30348-5788 <i>Fraud alert:</i> P.O. Box 105069 Atlanta, GA 30348-5069	Experian 1-888-397-3742 experian.com/help <i>Credit report:</i> P.O. Box 2002 Allen, TX 75013-9701 <i>Fraud alert and credit freeze:</i> P.O. Box 9554 Allen, TX 75013	TransUnion 1-888-909-8872 transunion.com/credit-help <i>Credit report:</i> P.O. Box 1000 Chester, PA 19016 <i>Fraud alert:</i> P.O. Box 2000 Chester, PA 19016 <i>Credit freeze:</i> P.O. Box 160 Woodlyn, PA 19094
---	---	--

Report Incidents. If you detect any unauthorized activity in your accounts, 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 incidents of identity theft to the appropriate law enforcement authorities, including local law enforcement, your state attorney general, and the Federal Trade Commission (FTC). To report identity theft to the FTC, contact: Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-438-4338. Complaints filed with the FTC will be added to the FTC's Consumer Sentinel database, which is made available to law enforcement agencies.

Consider Placing a Fraud Alert on Your Credit File. You may want to consider placing a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. As soon as one credit reporting agency confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year, unless you choose to remove it sooner. You can renew it after one year.

Consider Placing a Credit Freeze on Your Credit File. You may also want to consider placing a free credit freeze (also called a security freeze). A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. You may be required to provide the credit bureau with personal information including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued ID card, and a recent utility bill, bank statement, or insurance statement. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it. There is no charge to request a freeze or to remove a freeze.

Take Advantage of Additional Free Resources on Identity Theft. Your state attorney general and the FTC can provide additional information about identity theft, fraud alert, and credit freezes. Information from the FTC is available at www.ftc.gov/idtheft and www.identifytheft.gov. You can also contact the FTC for more information at: Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-382-4357.

For DC Residents. You have the right to obtain a credit freeze, as described above. You can obtain information about preventing identity theft from the FTC, as described above, or the DC Attorney General at: 400 6th Street, NW, Washington, DC 20001, www.oag.dc.gov, 202-727-3400.

For Iowa Residents. You can contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General's Office at: Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, 515-281-5926, 1-888-777-4590 (toll free in Iowa).

For Maryland Residents. You can obtain information about the steps you can take to avoid identity theft from the FTC, as described above, or the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023 (toll-free).

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

For New York Residents. You can obtain information about preventing identity theft from the New York Attorney General at: <https://ag.ny.gov>, 1-800-771-7755 (toll-free). You can also obtain information about preventing identity theft from the New York Department of State Division of Consumer Protection at: www.dos.ny.gov/consumer-protection, 1-800-697-1220 (toll-free).

For North Carolina Residents. You can obtain information about preventing identity theft from the FTC, as described above, or the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226 (toll-free).

For Oregon Residents. You can contact local law enforcement, the Oregon Attorney General's Office, or the FTC to report suspected incidents of identity theft. You can contact the Oregon Attorney General's Office at: 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, 1-877-877-9392 (toll-free).

For Rhode Island Residents. Five individuals in Rhode Island were affected by this incident. You have the right to file or obtain a police report. You also have the right to obtain a credit freeze, as described above. You can obtain information from the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.