

[CLIENT LOGO]
<<RETURN ADDRESS>>
<<CITY>>,<<STATE>> <<ZIP>>

<DATE>

Name
Address 1
Address 2
City, State, Zip Code

Re: NOTICE OF DATA SECURITY INCIDENT

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

We value our relationship with you and your confidence in entrusting your business to us. In that same confidence, we share the information below about a recent security incident that Set Forth, Inc. (“Forth”) experienced. This letter provides you with information about what occurred, the steps Forth has taken in response, and how Forth will support you with any additional steps that need to be taken. Our goal is to ensure this matter is resolved in a thorough and thoughtful manner, and with as little burden on you and your operation as possible.

Who is Set Forth?

Forth provides online account administration services to consumers enrolled in debt relief programs. In addition to providing consumer services, Forth has relationships with business-to-business partners such as Centrex, Inc. (“Centrex”). Receipt of this letter may be confusing for those who have not been direct customers of Forth. You may be receiving this letter if you were a customer or have done business with Centrex, Inc.

What Happened?

On May 21, 2024, Forth identified suspicious activity on its system, and immediately implemented our incident response protocols, and engaged independent computer forensic specialists to investigate the activity and determine what, if any, data may have been impacted. The investigation determined that personal information belonging to yourself, a spouse, co-applicant, or dependent may have been accessed during the incident. While there is no evidence to suggest that your information has been misused, we wanted to make you aware of this incident out of an abundance of caution.

What Information Was Involved?

From our review, it appears that your name, address, date of birth, and social security number may have been affected.

What We Are Doing:

Data security is one of our highest priorities. We want to assure you that we are taking steps to prevent a similar incident from happening in the future. Since the incident, we deployed enhanced endpoint monitoring software, performed a global password reset, and implemented additional security controls. In

addition to these measures, we are offering identity theft protection services through Cyberscout for 12 months. With this protection, Cyberscout will help you resolve issues if your identity is compromised.

What You Can Do:

<<Vendor Instructions of enrollment>>

This letter also provides other precautionary measures you can take to protect your information. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. 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.

For More Information:

We sincerely apologize for any inconvenience this incident may cause you. If you have questions, please call [TFN] Monday through Friday from 9 am – 9 pm Eastern Time. Please have the membership number ready.

Sincerely,

Set Forth, Inc.

Recommended Steps to help Protect your Information

1. Website and Enrollment.

<<Insert credit monitoring enrollment instructions>>

2. 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.

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.

3. 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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.

4. 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.

5. 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.

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. A total of [XX] Rhode Island residents were notified of this incident.

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