C/O IDX
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-726-0947
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXX>>

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

February 19, 2021

Re: Notice of Data Security Incident

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

I am writing to inform you of a data security incident experienced by Team One Adjusting Services, LLC ("Team One"), that may have involved your personal information. At Team One, we take the privacy and security of your information very seriously. This is why I am notifying you about the incident, offering you credit and identity monitoring services, and providing you with information about steps you can take to help protect your information.

What Happened? On January 24, 2021, Team One became aware of a possible data security incident involving our computer network. We immediately began an investigation and hired independent computer forensic investigators to help us determine what happened. That investigation confirmed that we experienced a malware attack and an unauthorized person may have accessed files or information stored on our network. On February 9, 2021, the investigation determined that some of your personal information may have been accessed by the unauthorized person.

What Information Was Involved? Based on our investigation, the information that may have been accessed may include your name, date of birth, Social Security number, driver's license number, passport number and financial account number.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. In addition, we are providing you with information about steps you can take to help protect your personal information, and we are offering you complimentary credit monitoring identity recovery services for <<membership offering length>> months through IDX as described below.

What You Can Do: You can follow the recommendations included with this letter to protect your personal information. I encourage you to enroll in the identity monitoring services Team One is offering to protect your personal information. To enroll, please visit https://app.myidcare.com/account-creation/protect or call 1-833-726-0947 and provide your enrollment code found above. Your <<membership offering length>> months of services will include credit monitoring, dark web monitoring, identity theft insurance and fully managed identity recovery.

To receive credit services, you must be over the age of 18, and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Additional information describing your services is included with this letter. Please note you must enroll by May 19, 2021.

For More Information: If you have any questions about this letter, please call 1-833-726-0947 Monday through Friday from 8am to 8pm Central Time.

Sincerely,

Eric Shaw
President

STEPS YOU CAN TAKE TO FURTHER 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 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 (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 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:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9701	P.O. Box 740241	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	866-349-5191	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

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 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. 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.

Security Freeze: Under U.S. law, 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.

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 at **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, D.C. 20580, or online at consumer.ftc.gov and www.ftc.gov/idtheft, or to the Attorney General in your state. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
Bureau of Internet and Technology Resources	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
28 Liberty Street	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
New York, NY 10005	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
ifraud@ag.ny.gov	410-528-8662	1-877-566-7226	401-274-4400
1-212-416-8433			

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 others. 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.

Review your Tax Filings: If you detect any suspicious activity relating to your tax filings, we encourage you to complete IRS Form 14039, Identity Theft Affidavit, which you can obtain at http://www.irs.gov/pub/irs-pdf/f14039.pdf. If you

have other identity theft / tax related issues, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. You should be especially aware of any requests, calls, emails, letters, or other questions about your financial accounts or from individuals purporting to be from the IRS or other entities from whom you would not be expecting contact. If you receive any type of unexpected request for personal information, you should not provide that information and instead contact the organization by phone to verify the request is legitimate.