Justworks, Inc.
P.O. Box 7119, Church Street Station
New York, NY 10008

June 9, 2023

[]

To Enroll, Please Call:
1-800-939-4170

Or Visit:
https://app.idx.us/account-creation/protect

Enrollment Code: []

Dear [],

We are writing to follow up on a security matter involving your Justworks user account, due to new information developed in a follow up detailed investigation.

As you are aware, there was recently suspicious activity on your account. Fortunately, account security detected and recovered from the compromise of your login credentials without any misdirection of any funds. Steps to resecure your account and validate your direct deposit information have been taken by Justworks.

We are taking this account compromise seriously. We retained a third-party forensic firm to assist us. We are reaching back out to you because this review indicated that your social security number was viewed during the time frame when your account was compromised. We are writing today to provide you with two (2) years of complimentary identity theft and credit monitoring services.

What Happened

Our investigation determined that your Justworks account was compromised on [] between [] and [], as a result, an unauthorized user gained access to your personal Justworks account. During this time some of your personal information was also compromised. The unauthorized user used your compromised credentials to change the bank account designated to receive your direct deposit, presumably in an attempt to divert funds to the bad actor's bank account. Our detailed log review indicates that when the unauthorized user accessed your personal Justworks account, your social security number was viewed.

What Information Was Involved

The information associated with your Justworks account included your name, address, email address, job information, social security number, original bank account details, and other profile information, such as your date of birth and emergency contact information. Social security number is masked, but was viewed by the unauthorized user who misused your credentials, according to log data.

What We Are Doing

To reduce the risk that your information may be used for unintended purposes, we are offering you credit monitoring and identity theft protection and have taken steps that will protect you, as follows:

- Promptly upon discovering the unauthorized access, Justworks sought and confirmed the removal of the phishing site from the web, alerted you to the need to reset your account password, and new multi factor authentication tokens were issued.

- To help protect your identity, Justworks is offering you complimentary 24-month identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 24-months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to remain vigilant by reviewing Justworks and financial account statements regularly and monitoring your consumer credit reports for suspicious activity. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. The U.S. Federal Trade Commission provides further guidance on steps you can take to protect your personal information, which you can access online at https://www.identitytheft.gov. Additional information on steps that you can take to protect your identity is attached to this letter. We encourage you to review these steps and to take appropriate action to prevent any misuse of your information.

Justworks requires multi-factor authentication on all Justworks accounts, and we always strongly recommend using an authenticator app as it's the most secure delivery method. Instructions are available here: https://help.justworks.com/hc/en-us/articles/360004534471-Multi-Factor-Authentication. While Justworks has already confirmed that passwords affected by this incident were reset, you can always change your password by following the instructions at the following link: https://secure.justworks.com/password_reset.

We encourage you to contact IDX with any questions you have and enroll in the free identity protection services by going to https://app.idx.us/account-creation/protect or calling 1-800-939-4170 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday 9 am - 9 pm Eastern Time. Please note the deadline to enroll is September 9, 2023.

Because of the sensitivity of the information at issue, we encourage you to take full advantage of this service offering.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-800-939-4170 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have regarding this matter.

Sincerely,

Yabing Wang
VP, Information Security

(Enclosure)

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. 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.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

5**. 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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	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.

6. 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.

7. 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.

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.

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.

Justworks

Justworks, Inc.
P.O. Box 7119, Church Street Station
New York, NY 10008

June 9, 2023

[]

To Enroll, Please Call:
1-800-939-4170

Or Visit:
https://app.idx.us/account-creation/protect

Enrollment Code: []

Dear [],

We are writing to provide notice of a recent security matter relating to personal information housed within your Justworks account.

On [] another employee at your company that has an administrative-level Justworks account had suspicious activity associated with their account.

We are taking this account compromise seriously. We retained a third-party forensic firm to assist us. We are reaching out to you because this review indicated that your social security number was viewed during the time frame when the administrator's account was compromised. We are writing today to provide you with two (2) years of complimentary identity theft and credit monitoring services.

What Happened

Our investigation determined that on [] between [] and [] an unauthorized user gained access to the Justworks account of an administrator at your company. Our detailed log review indicates that when the unauthorized user accessed the administrator's Justworks account, your social security number was viewed.

Please note that your personal Justworks account was not compromised. There was only suspicious activity associated with the administrator's account. However, within the administrator's account, your social security number was viewed, according to our forensic evidence. Justworks has alerted the administrator that they need to reset their account password.

What Information Was Involved

The information that was viewed by the unauthorized user included your name, address, email address, job information, social security number, and other profile information, such as your date of birth and emergency contact information. Social security number is masked, but was viewed by the unauthorized user who misused the administrator's credentials, according to log data.

What We Are Doing

To reduce the risk that your information may be used for unintended purposes, we are offering you credit monitoring and identity theft protection and have taken steps that will protect you, as follows:

- Promptly upon discovering the unauthorized access, Justworks sought and confirmed the removal of the phishing site from the web, alerted your company's administrator of the need to reset their account password, and new multi factor authentication tokens were issued.

- To help protect your identity, Justworks is offering you complimentary 24-month identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 24-months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to remain vigilant by reviewing Justworks and financial account statements regularly and monitoring your consumer credit reports for suspicious activity. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. The U.S. Federal Trade Commission provides further guidance on steps you can take to protect your personal information, which you can access online at https://www.identitytheft.gov. Additional information on steps that you can take to protect your identity is attached to this letter. We encourage you to review these steps and to take appropriate action to prevent any misuse of your information.

Justworks requires multi-factor authentication security features on all Justworks accounts, and we always strongly recommend using an authenticator app as it's the most secure delivery method. Instructions are available here:https://help.justworks.com/hc/en-us/articles/360004534471-Multi-Factor-Authentication. While Justworks has already confirmed that passwords affected by this incident were reset, you can always change your password by following the instructions at the following link: https://secure.justworks.com/password_reset.

We encourage you to contact IDX with any questions and enroll in the free identity protection services by going to https://app.idx.us/account-creation/protect or calling 1-800-939-4170 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday 9 am - 9 pm Eastern Time. Please note the deadline to enroll is September 9, 2023.

Because of the sensitivity of the information at issue, we encourage you to take full advantage of this service offering.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-800-939-4170 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have regarding this matter.

Sincerely,

Yabing Wang
VP, Information Security

(Enclosure)

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4**. 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.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

5. 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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	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.

6. 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.

7. 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.

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.

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.