



C/O ID Experts
 10300 SW Greenburg Rd., Suite 570
 Portland, OR 97007

To Enroll, Please Call:
 1-800-939-4170
 Or Visit:
<https://app.myidcare.com/account-creation/protect>
 Enrollment Code: <<XXXXXXXXXX>>

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

October 9, 2020

Re: Notice of Data Security Incident

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

We had hoped there would never be a need for this type of letter. Unfortunately, we are writing to provide you with information about a recent data security incident that may have involved your personal information. At One Workplace, we take the privacy and security of our employees’ and their dependents’ information very seriously. That is why we are sending you this letter to tell you about the incident, offering you credit monitoring and identity monitoring services, and providing you with information, resources and steps you can take to help protect your personal information.

What Happened? On August 14, 2020, One Workplace was alerted to suspicious activity on our computer network. We hired cybersecurity experts and a computer forensic investigator to help us investigate the incident, ensure the safety of our environment, and confirm whether anyone’s personal information was impacted. The investigation confirmed that we were the victim of a ransomware attack, and an unauthorized individual had gained access to our network. Based on the investigation, the attacker viewed and removed some data stored in the system. On September 17, 2020, we confirmed that the data viewed or taken by the attacker included employees’ personal information.

What Information Was Involved? The potentially impacted information includes your name, Social Security number, Driver’s license or government issued identification number, and, medical or health insurance information.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. We also notified the FBI and will fully cooperate with any law enforcement investigation. In addition, we are offering you identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do. We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is January 8, 2021.

At this time, we are unaware of the misuse of any of your information. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information:

Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call 1-800-939-4170, Monday through Friday from 6 am - 6 pm Pacific Time.

We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Mark Baker', with a stylized, cursive script.

Mark Baker
Chief Operating Officer

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 and review 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 should also 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 <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 also contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.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: You have the right to put a security freeze on your credit file. 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. There is no charge to place, lift or remove the security freeze. 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 or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338. 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

Bureau of Internet and
Technology Resources
28 Liberty Street
New York, NY 10005
ifraud@ag.ny.gov
1-212-416-8433

**Maryland Attorney
General**

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

**North Carolina Attorney
General**

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

**Rhode Island
Attorney General**

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies may be found below.