

April 20, 2020

NAME
ADDR 1
CITY, ST ZIP

Subject: **Notice of Data Breach**

Dear **SALUTATION**:

As the former service provider for your 401K retirement plan with KDW Automotive, Wells Fargo is writing on behalf of KDW Automotive to inform you of an incident Wells Fargo experienced that may affect the security of your personal information. We apologize for any concern this may cause and take this matter seriously. Below, we've provided information about the incident and resources available to you to help protect your information.

What happened?

On December 23rd, 2019, Wells Fargo learned that an email, which included a file with some of your personal information intended for your current 401K service provider, was mistakenly sent to another financial institution and one of our business customers on November 6, 2019. Upon discovering the error, the recipients notified Wells Fargo and confirmed deleting the information. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What information was involved?

The personal information involved included your name and social security number.

What we are doing

We are offering you a complimentary two-year subscription to Experian IdentityWorksSM, a credit monitoring and identity theft protection service provided by Experian[®].

If you choose to accept this offer, enroll online at www.experianidworks.com/3bplus or by calling **1-877-890-9332**, Monday through Friday, 8:00 a.m. - 8:00 p.m. Central Time and Saturday/Sunday, 10:00 a.m. - 7:00 p.m. Central Time by **June 22, 2020**. By law, we cannot enroll for you.

When you enroll, you will be asked to provide the following information:

Activation Code: 

Engagement Number: 

Your social security number, email address, mailing address, phone number, and date of birth

At the end of your free subscription, it will be canceled and you will not be billed. Please see additional details enclosed.



What you can do

We have enclosed *Tips to Safeguard Personal Information*, and additional helpful tips, which we encourage you to read and follow.

Additionally, we encourage you to take advantage of the Experian IdentityWorksSM subscription we are offering you.

For more information

We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line to respond to questions at 1-855-907-2087. This response line is staffed with professionals familiar with this incident and knowledge on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time.

Sincerely,



Patrick Pruden
Institutional Retirement and Trust Operations Manager

Enclosure



Tips to Safeguard Personal Information

Protecting your accounts:

- Monitor your account statements often (even daily in online banking) to review all charges and transactions. Contact us immediately at 1-800-TO-WELLS (1-800-869-3557) 24 hours a day, and 7 days a week, if you see discrepancies or unauthorized activity on your Wells Fargo accounts. We will carefully review them for reimbursement in accordance with our policies.
- If available, consider placing password protection on your Wells Fargo accounts, and do not use any part of your social security number as the username or password. To find out if password protection is available for your accounts, visit any Wells Fargo branch. Or we can help you close these accounts and transfer the money to new accounts. For this option, please call us at 1-800-TO-WELLS (1-800-869-3557), 24 hours a day, and 7 days a week, or visit any Wells Fargo branch.
- For more tips on how to protect your Wells Fargo accounts, please visit www.wellsfargo.com/privacy_security
- Do not write down or share your Personal Identification Number (PIN) number or passwords with anyone.
- If you receive suspicious emails that claim to be from Wells Fargo, forward them to reportphish@wellsfargo.com and then delete them.
- If you have accounts at other financial institutions, please notify them and they can advise you on additional steps to take.
- If your user name or email address, with a password or security question and answer that would permit access to an online account were involved, promptly change you user name or password and security question or answer, as applicable, or take other appropriate steps to protect online accounts for which you use the same user name or email address and password or security question and answer.

Protecting your identity:

- Place a 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. Call any one of the three major credit bureaus listed on the back of this page. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. This provides a significant layer of protection; however, it may limit your ability to get "instant credit" such as the offers often available at retail branches.
- Check your credit report to ensure all your information is correct. You can obtain a free credit report from each of the three major credit bureaus every 12 months by visiting www.annualcreditreport.com or calling 1-877-322-8228.
- If you believe you are a victim of identity theft, report it to your local law enforcement agency and to the Federal Trade Commission (FTC) or your state Attorney General.
- You also may want to consider placing a freeze on your credit file. A credit freeze means potential creditors cannot get your credit report and makes it less likely that an identity thief can open new accounts in your name. To place a freeze on your credit you can contact the nationwide credit bureaus. You can freeze your credit for free, but you'll need to supply your name, address, date of birth, social security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. To lift the freeze, you will need to contact the credit bureaus again.
- Information on how to contact the major credit bureaus, the FTC and Attorneys General can be found on the back of this page.

Additional Helpful Tips

Below are additional helpful tips you may want to consider to protect your personal information.

Sign up for free credit monitoring. Features of Experian IdentityWorksSM include:

Experian[®] credit report at signup:

See what information is associated with your credit file. Daily credit reports are available for online members only.*

Credit Monitoring:

Actively monitors Experian[®], Equifax[®] and TransUnion[®] files for indicators of fraud.

Internet Surveillance:

Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.

Identity Restoration:

Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.

Up to \$1 Million Identity Theft Insurance:

Provides coverage for certain costs and unauthorized electronic fund transfers.**

Experian's IdentityWorks ExtendCARETM:

You receive the same high level of Identity Restoration support even after your Experian IdentityWorksSM membership has expired.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage.

Contact major credit bureaus:

To get useful information about protecting your credit, including information about fraud alerts, security freezes, or other steps you can take to protect yourself from fraud and identity theft. To obtain an annual free copy of your credit report, visit annualcreditreport.com, or call toll-free at 1-877-322-8228. Credit bureau contact details are provided below.

Equifax[®]:

1-800-525-6285 or
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian[®]:

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

TransUnion[®]:

1-800-680-7289 or
www.transunion.com
P.O. Box 6790
Fullerton, CA 92634

Visit the Federal Trade Commission website:

The Federal Trade Commission (FTC) has helpful information about how to avoid and protect against identity theft.

FTC Consumer Response Center
600 Pennsylvania Avenue, NW, H-130
Washington, DC 20580
1-877-438-4338
www.identitytheft.gov

Contact your Attorney General:

For more information about preventing and managing identity theft, you can contact the Attorney General's office in the state in which you reside. Contact information for the Attorney General's office in additional states can be found at www.naag.org.

For Maryland:

200 St. Paul Place
Baltimore, MD 21202-2202
1-888-743-0023
www.marylandattorneygeneral.gov

For North Carolina:

Dept. of Justice, P.O. Box 629
Raleigh, NC 27602-0629
919-716-6400
www.ncdoj.gov

For Rhode Island:

150 S. Main St.
Providence, RI 02903
401-274-4400
www.riag.ri.gov

