

BRAD C. MOODY
Direct Dial: 601.351.2420
Direct Fax: 601.592.2420
E-Mail Address: bmoody@bakerdonelson.com

April 10, 2020

Attorney General Gordon J. MacDonald
Office of New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: *U.S. Xpress, Inc. - Notice of Data Incident*

Dear Attorney General MacDonald:

I serve as outside legal counsel to U.S. Xpress Enterprises, Inc. (“USX”), which is a publicly traded company operating two national truckload carriers that provide services throughout the U.S. and across North America. USX’s principal place of business is located at 4080 Jenkins Road, Chattanooga, TN 37421.

This correspondence is to notify you of a recent security event involving the potential compromise of business email accounts resulting from a phishing scam.¹ USX promptly conducted an extensive investigation and blocked the unauthorized access.

Because the Personally Identifiable Information (“PII”) for some individuals was at risk during the incident, in an abundance of caution, notification letters were sent via U.S. Mail to 16 residents of your State on or about April 10, 2020. The data elements for affected residents included a combination of first and last names with a driver’s license number, Social Security number or financial account number. A sample notification letter is enclosed for your reference and includes -

- A description of the security event;
- Steps taken to investigate;
- Steps taken to mitigate any potential harm to consumers;
- Instructions for activation of 1 year of free identity theft protection services that includes credit monitoring and a \$1 million insurance reimbursement policy to all consumers who received notification;

¹ Law enforcement has not been alerted to this incident.

- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this event, etc.

Additional steps taken in response to the incident include the following:

- Activated multi-factor authentication for all email users by October 24, 2019;
- Provided individuals with free credit monitoring; and
- Trained or retrained email users to reinforce security awareness.

USX is fully committed to protecting consumer privacy and the confidentiality of personal information. We will follow-up this correspondence with any forms or other documents that may need to be completed. Please contact me if you require any additional information regarding this incident.

Best regards,

BAKER, DONELSON, BEARMAN,
CALDWELL & BERKOWITZ, PC


Brad C. Moody

Enclosure:

Exhibit 1: Sample Notification Letter sent to 16 residents



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

U.S. Xpress Enterprises, Inc. ("USX") is notifying you of an incident that may have involved your personal information.

Recently, an employee of one of our subsidiaries fell victim to an email phishing scam by opening an attachment/link containing malware - which eventually allowed unauthorized access to the individual's email account. The email account accessed contained some of your personal information.

USX investigated this incident internally and the unauthorized access was promptly blocked. USX also engaged outside technical experts to further investigate in order to evaluate the full nature and scope of any potential access.

On October 18, 2019, we were alerted by the outside experts as to the extent of the intrusion, and that the unauthorized access may have first occurred in September 2019. From there, we then conducted an extensive document review (which involved the tedious process of hand reviewing individual emails and attachments) in order to be able to identify individuals who potentially needed to be notified of this incident. These same emails were also reviewed to obtain names for use in notification.

On February 21, 2020 we were provided the listing of affected individuals, and from that listing we were first alerted that the information potentially involved included your <<b2b_text_3 (Impacted Data)>>. From there, we began the process of notifying potentially-affected individuals, including compiling mailing addresses.

We recommend you take precautions, and we are offering you one (1) year of **free** credit monitoring and \$1 million in identity theft insurance through Experian - to give you peace of mind. **You must activate the Experian product by the activation date in order for it to be effective. The activation instructions are included with this notification.** We also have included some additional steps that you can take to help protect yourself, as you deem appropriate.

For more information about this incident, call toll-free 1-800-737-4152 between 8:00 a.m. - 5:30 p.m. Central Time Monday - Friday (excluding some U.S. holidays). USX is continuing to take steps to enhance its security measures to help prevent something like this from happening in the future. We are fully committed to safeguarding your personal information and sincerely apologize for any concern this incident may have caused you.

Sincerely,

U.S. Xpress Enterprises, Inc.

Nathan Harwell
Chief Legal Officer

STEPS YOU CAN TAKE

Below is information on steps you can take to protect yourself.

ACTIVATE Your FREE Experian IdentityWorks product NOW in Three Easy Steps. To help protect your identity, we are offering you a complimentary one-year membership of Experian's® IdentityWorks® product. This product helps detect possible future misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks Alert is completely free to you and enrolling in this program will not hurt your credit score.

1. ENSURE That You Enroll By: <<b2b_text_1 (Date)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE Your Activation Code: <<Member ID>>

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement number <<b2b_text_2 (Engagement Code)>>. A credit card is not required for enrollment. Once your IdentityWorks membership is activated, you will receive the following features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only¹.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **\$1 Million Identity Theft Insurance:**² Provides coverage for certain costs and unauthorized electronic fund transfers.

You must activate your membership by the enrollment date (noted above) by enrolling at <https://www.experianidworks.com/3bcredit> or calling 877-288-8057 to register your activation code above in order for this service to be activated.

Once your enrollment in IdentityWorks is complete, carefully review your credit report for inaccurate or suspicious items. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer team at 877-288-8057.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² 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. Coverage may not be available in all jurisdictions.

Below are additional actions you may take, if you feel it is necessary.

FREEZE YOUR CREDIT FILE. You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze.

To place a security freeze on your credit report, contact each of the three major consumer reporting agencies using the contact information listed below:

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

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

TransUnion

P.O. Box 2000
Chester, PA 19022
1-800-680-7289
www.transunion.com

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.), Social Security number, and date of birth;
- If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the freeze.

PLACE FRAUD ALERTS ON YOUR CREDIT FILE. As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.

REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS, & REPORT FRAUD. Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity. Report suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor and law enforcement. (For Oregon & Iowa residents: Report any suspected identity theft to law enforcement, Federal Trade Commission, and your State Attorney General.)

ORDER YOUR FREE ANNUAL CREDIT REPORTS. Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

POLICE REPORT: You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it.

OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC / STATE ATTORNEY GENERAL. Go to <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html>. The Federal Trade Commission also provides information at www.ftc.gov/idtheft. The FTC can be reached by phone: 1-877-438-4338; TTY: 1-866-653-4261 or by writing: 600 Pennsylvania Ave., NW, Washington, D.C. 20580. Your State Attorney General also may provide information. (For Maryland residents: You may contact Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023. For North Carolina residents: You may contact North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226. For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 1-401-274-4400.

FILE YOUR TAXES QUICKLY AND SUBMIT IRS FORM 14039. If you believe you are at risk for taxpayer refund fraud, the IRS suggests you file your income taxes quickly. Additionally, if you are an actual or potential victim of identity theft, the IRS suggests you give them notice by submitting IRS Form 14039 (Identity Theft Affidavit). This form will allow the IRS to flag your taxpayer account to alert them of any suspicious activity. Form 14039 may be found at <https://www.irs.gov/pub/irs-pdf/f14039.pdf>.

FAIR CREDIT REPORTING ACT: You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Please note that identity theft victims and active duty military personnel may have additional rights under the FCRA.

PROTECT YOURSELF FROM PHISHING SCAMS. Learn to recognize phishing emails. Do not open emails from unknown senders, and be sure not to click on strange links or attachments. Never enter your username and password without verifying the legitimacy of the request by contacting the sender by telephone or other methods. Replying to the email is not a safe way to confirm. Visit <https://www.consumer.ftc.gov/articles/0003-phishing> for more information on these types of scams.