



Dear Attorney General Brown,

We are contacting you on behalf of United Bridge Partners (“UBP”) to provide notification of a data security incident that may have affected the security of personal information of three (3) Maryland residents.

On May 20, 2023, we were notified by a vendor that it experienced a potential compromise of a server which stored our customer account information. Threat Actors deployed ransomware after gaining unauthorized access to the networks. On July 8, 2023, the vendor discovered that some data records had been exfiltrated and posted on the darkweb. Our vendor reported the compromise to law enforcement, initiated its security incident response protocols and launched an investigation to determine the nature and scope of the incident. That investigation included reviewing the records contained on the compromised server. Based on their review of the records, it was determined that some impacted records contained personal information, such as: name, Social Security number, driver’s license number and/or bank account number.

After we were notified of the possibility of an incident, we immediately took steps to determine the customers whose information was obtained and what that personal information was. The process of going through all the effected individuals manually was labor intensive and time consuming. As soon as we determined the individuals who needed to be notified, we began drafting the notifications to be sent out. Given that 31.3 million vehicles have traveled on the South Norfolk Jordan Bridge since our original opening, we are, in some respects, fortunate and relieved that such a small percentage of our travelers information was compromised due to this incident. To prevent security incidents from happening again in the future, we are working with our vendors and requiring them to implement additional security measures that are designed to prevent a recurrence of such an incident and to protect the privacy of our valued customers. We are continuing to work closely with the vendor to understand what was done to assess and prevent any future threats. We are also working with external experts to assess our security controls and those of our vendors and suppliers.

Please find attached as Exhibit A the sample letter that we will be sending to all affected individuals. At UBP, we take the privacy of our customers very seriously, which is why we are additionally offering all affected individuals free credit monitoring for one (1) year.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Kevin Crum".

Kevin Crum
General Manager
South Norfolk Jordan Bridge
1001 Scenic Parkway, Suite 203
Chesapeake, VA 23323
(757) 932-8515



[Name]
[Address]
[City, State Zip]

Re: United Bridge Partners – Data Compromise

Dear [Name]:

United Bridge Partners (“UBP”) values and respects the privacy of your information, which is why we are writing to let you know about a data security incident that involves your personal information.

WHAT HAPPENED?

On May 20, 2023, we were notified by a vendor that it experienced a potential compromise of a server which stored our customer account information. On July 8, 2023, the vendor discovered that some data records had been posted on the darkweb. Our vendor reported the compromise to law enforcement, initiated its security incident response protocols and launched an investigation to determine the nature and scope of the incident. That investigation included reviewing the records contained on the compromised server.

WHAT INFORMATION WAS INVOLVED?

Based on a review, some impacted records contained personal information, such as name, Social Security number, driver’s license number and/or bank account number.

WHAT WE ARE DOING

After we were notified of the possibility of an incident, we began the manual and labor-intensive process to determine the customers whose information may have obtained and what that personal information was. As soon as we determined the individuals who needed to be notified, we began drafting the notifications to be sent out. To help prevent security incidents in the future, we are working with our vendors to implement additional security measures that are designed to prevent a recurrence of such an incident and to protect the privacy of our valued customers. We are also continuing to work closely with our vendor to assess and prevent any future threats. We are also working with external experts to assess our security controls and those of our vendors and suppliers.

WHAT YOU CAN DO

Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information, and how to receive free identity protection services for one year.

FOR MORE INFORMATION

UBP is continuing to take steps to enhance its security measures and to ensure that its vendors also do the same to help prevent incidents such as this from happening. We are fully committed to protecting your personal information.

UBP has arranged with Experian to provide you with identity theft protection services for one (1) year, at no cost to you. Please see the enclosed information on how you can obtain your complimentary identity theft protection.

For further information or assistance, please contact our customer care team at:

Phone:

(855) 690-7652 (select option 0) between 8:00 am and 6:00 pm EST Monday through Friday.

Address:

South Norfolk Jordan Bridge
1001 Scenic Parkway, Suite 203
Chesapeake, VA 23323

Best regards,

A handwritten signature in black ink, appearing to read 'Kevin Crum', with a stylized, flowing script.

Kevin Crum
General Manager
South Norfolk Jordan Bridge

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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting 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 access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

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 www.annualcreditreport.com.

Identity Theft Protection Services

In addition, UBP has arranged with Experian to provide you with identity theft protection services for one (1) year, at no cost to you. This product provides you with superior identity detection and resolution of identity theft.

To take advantage of this offer, you must enroll within 90 days from receipt of this letter.

To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: [enrollment end date – 90 days from letter]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://portal.experianidworks.com/enrollment/1?RTN=90000443>
- Provide your **activation code: [code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-888-397-3742 by **[enrollment end date]**. Be prepared to provide engagement number **[engagement #]** as proof of eligibility for the identity restoration services by Experian.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://consumer.ftc.gov/identity-theft-and-online-security>.

For more information, please visit [IdentityTheft.gov](https://www.identitytheft.gov) or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.