

BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Joseph L. Bruemmer
direct dial: 513.929.3410
jbruemmer@bakerlaw.com

July 21, 2022

VIA E-MAIL (NDAG@ND.GOV)

Office of the Attorney General
State Capitol
600 E. Boulevard Ave.
Department 125
Bismarck, ND 58505

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Sixt Rent-a-Car, LLC (“Sixt”), to notify your office of a cybersecurity incident. Sixt’s headquarters are located at 1501 NW 49th Street, Suite 100 Fort Lauderdale, Florida 33309-3723.

Sixt’s parent company recently identified unusual network activity that caused certain systems in its network to become unavailable. It immediately began an investigation, a cybersecurity firm was engaged, and measures were taken to address the incident and to restore the systems. The evidence showed that there was unauthorized activity in the company network between April 27, 2022 and May 1, 2022. During that time, an unauthorized party obtained files stored on Sixt’s file server. Sixt conducted a careful review of those files and, on June 2, 2022, determined that the files contained information belonging to four North Dakota residents, including their names and one or more of the following data elements: Social Security number, driver’s license number or state identification card number, passport number or other government-issued identification number, financial account number used for direct deposit, health insurance number, health information, and date of birth. In addition, on June 20, 2022, determined that the files contained the names and dates of birth of 345 North Dakota residents. This was the date on which Sixt determined that the incident involved information concerning more than 250 North Dakota residents.

On July 6, 2022, Sixt mailed notification letters via United States Postal Service First-Class mail to the four North Dakota residents whose information was identified on June 2, 2022. On July

July 21, 2022

Page 2

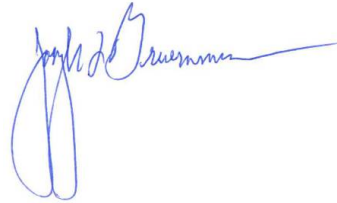
21, 2022, Sixt will mail notification letters via United States Postal Service First-Class mail to the 345 North Dakota residents whose information was identified on June 20, 2022, in accordance with N.D. Cent. Code § 51-30-01. A copy of the notification letter is enclosed. Sixt is offering the residents whose Social Security number, driver's license number, or state identification card number was involved a complimentary one-year membership to credit monitoring and identity theft protection services. Sixt also has established a dedicated, toll-free call center that individuals can call to obtain more information regarding the incident.

To help prevent something like this from happening again, Sixt is working with its parent company to further enhance the security of their networks.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Joseph L. Bruemmer

A handwritten signature in blue ink, appearing to read "Joseph L. Bruemmer", with a long horizontal flourish extending to the right.

Partner

Sixt Rent-A-Car
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



L-1

July 21, 2022

Dear [REDACTED]

Sixt understands the importance of protecting information. We are writing to inform you that we recently identified and addressed a security incident that involved some of your information. This notice explains the incident, the measures we have taken in response, and some additional steps you can consider taking.

Our parent company identified unusual network activity that caused certain systems in its network to become unavailable. It immediately began an investigation, a cybersecurity firm was engaged, and measures were taken to address the incident and to restore the systems.

The evidence showed that there was unauthorized activity in the company network between April 27, 2022 and May 1, 2022. During that time, an unauthorized party obtained files stored on our file server. We conducted a careful review of those files and, on June 20, 2022, determined that the files contained your name and date of birth.

We wanted to notify you of this incident and to assure you that we take it seriously. We encourage you to remain vigilant by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized activity to your financial institution. For more information on identity theft prevention and steps you can take to protect your information, please see the additional information provided in this letter.

We regret that this occurred and apologize for any inconvenience. To help prevent something like this from happening again, we are working with our parent company to further enhance the security of our networks. If you have additional questions, please call 800-426-5298 Monday through Friday, between 8:00 am and 5:00 pm, Eastern Time.

Sincerely,

Sixt

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.