Leader Bank
A STEP AHEAD

VIA CERTIFIED U.S. MAIL

June 6, 2017

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capital Street
Concord, NH 03301

Dear Sir/Madam:

I write to you on behalf of Leader Bank, N.A. ("Leader Bank") whose corporate offices are located at 180 Massachusetts Avenue, Arlington, Massachusetts, 02474, to notify you of a breach of security potentially involving the nonpublic personal information of up to twelve (12) New Hampshire residents.

NATURE OF THE SECURITY BREACH

On May 26, 2017, as the result of an Incident Response Team investigation regarding a customer's notification of multiple unauthorized ACH withdrawals from her checking account, Leader Bank, N.A. discovered a security vulnerability in its ZRent platform. ZRent is a proprietary service through which tenants and landlords can agree for the monthly payment of distribution of rent by ACH transfer. As the result of an intensive review of ZRent's files, servers and coding, as well as IP address access and account activity, Leader Bank determined that on December 30, 2016, a malicious actor was able to exploit the "upload picture" feature and upload a malicious file to the ZRent server. This program allowed the actor to access certain ZRent customer information as follows:

- In late January 2017, the actor used the program to download a backup database of ZRent customer information. However, all ZRent databases have bank routing and account numbers and social security and tax identification numbers encrypted, and Leader Bank's review did not provide any evidence or information that the encryption key was compromised or accessed by the actor. Accordingly, at this time Leader Bank does not believe that the nonpublic personal information in this specific database was compromised as a result of the incident.
- Between January and May 2017, the actor executed a series of commands via the malicious program in an attempt to decrypt and access specific fields of information for ZRent landlord customers one by one. Each field, such as account number and tax identification number, requires an individual command, and based on the total number of commands run, at this time Leader Bank does not believe that every nonpublic personal information field retained for ZRent landlords was accessed. However, Leader Bank cannot determine from its logs which landlords may have had their account information accessed.
- Thus, the landlords who had established a ZRent account prior to May 19, 2017 may have had their bank account numbers, dates of birth (if provided) and social security or tax identification numbers (if provided) compromised. However, Leader Bank did not collect social security or tax identification numbers or dates of birth in its ZRent platform for more than 60% of the landlords potentially impacted by this incident, so such information was not compromised for the majority of landlords.

At this time, Leader Bank does not believe or have information to suggest that the nonpublic personal information of any ZRent tenant customer was impacted by this incident.

180 Massachusetts Avenue, Arlington, MA 02474
Phone: 781-646-3900 • Fax: 781-646-3910
www.leaderbank.com

Leader Bank
A STEP AHEAD

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

As noted above, Leader Bank cannot determine the exact number of residents whose information was improperly accessed. To date, our investigation has not confirmed that any New Hampshire resident was definitively impacted; however, up to twelve (12) New Hampshire residents could have been impacted. By June 7, 2017, Leader Bank will send notices to all potentially impacted New Hampshire customers by United States mail. A sample copy of the notice provided is attached hereto. Although not all ZRent landlords had their information accessed in this breach, we believe it is appropriate to notify all potentially impacted residents to ensure they are aware of this situation and can take appropriate precautions. In addition, Leader Bank's ZRent team has begun personally calling all potentially impacted landlord customers to ensure they are aware of the situation and can take advantage of any services offered by the Bank.

STEPS TAKEN OR STEPS THAT WILL BE TAKEN RELATING TO THE INCIDENT

Safeguarding our customers' personal information is of the utmost importance to ZRent and Leader Bank. We took immediate responsive steps and implemented containment measures to prevent this unauthorized access to our system, as outlined below. Leader Bank has contacted the FBI regarding the specific losses and overall incident, including filing IC3 reports with the federal authorities. A copy of these IC3 reports can be provided upon request. Leader Bank has cooperated and will continue to cooperate with authorities to provide all information to identify these malicious actors. Please note that this notification was not delayed due to a law enforcement investigation.

As noted above, Leader Bank's Incident Response team, which included representatives from the Bank's IT, legal, compliance, security and affected business lines, to investigate and document the security breach and to ensure that all appropriate steps are taken. In particular, Leader Bank immediately quarantined all malicious or potentially malicious files and installed a software patch to ensure that malicious actors could not further utilize the upload picture feature. The Bank also immediately implemented several other security upgrades to the ZRent platform to prevent unauthorized access. Further, Leader Bank has established a plan of additional steps to be taken to ensure the vulnerability and security breach are properly addressed, including implementation of additional security features surrounding ZRent access as well as additional monitoring and logging.

To date, Leader Bank has determined that only nine specific ZRent customers had information used or likely used for fraudulent purposes, and there is no indication that any other ZRent landlord has had their nonpublic personal information used for fraudulent purposes. However, out of an abundance of caution and in order to help protect all potentially affected customers, Leader Bank will offer free credit monitoring and identity theft protection services from LifeLock for a period of one year to those ZRent landlords with information in the system prior to May 19, 2017. We will continue to monitor all ZRent systems and any Leader Bank accounts held by the affected ZRent landlord customers for any suspicious and unauthorized activity on an ongoing basis. Finally, Leader Bank will take all steps identified above to ensure the continued security of ZRent and its overall systems.

180 Massachusetts Avenue, Arlington, MA 02474
Phone: 781-646-3900 • Fax: 781-646-3910
www.leaderbank.com

Leader Bank and its ZRent team take its customers' privacy and its obligations under federal and state laws very seriously, and will assist the Attorney General in any way necessary. In the event Leader Bank gains any additional information that would require a revision or update to this notice, we will inform you of that updated information as soon as possible. If you require any further information or have any questions regarding the incident described herein, please do not hesitate to contact me by telephone at 781-641-7550 or bames@leaderbank.com.

Sincerely,

Brook Ames
General Counsel
Leader Bank, N.A.

Enclosure

cc: Sushil K. Tuli, President & CEO
John A. Fanciullo, EVP & COO
Jay Tuli, SVP of Retail Banking & ZRent

180 Massachusetts Avenue, Arlington, MA 02474
Phone: 781-646-3900 • Fax: 781-646-3910
www.leaderbank.com

Leader Bank
A STEP AHEAD

June 7, 2017

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

Dear [Name],

We are writing to notify you that Leader Bank's ZRent team became aware of a security vulnerability in which an incident of unauthorized access was detected. Specifically, we discovered on May 26, 2017 that a malicious program was uploaded to our system on December 30, 2016, resulting in periodic unauthorized access to the ZRent system between January and May 2017. This access may have compromised certain personal information belonging to our ZRent landlords, such as bank account information, social security or tax identification number (if provided) and date of birth (if provided). Although we do not know whether any individual's specific information was compromised, we believe there is a possibility that the personal information for some of the Landlords on the ZRent application owned by Leader Bank N.A. may have been attained during the period of January through May 2017.

Please note that we take this security issue extremely seriously. Our ZRent team immediately removed the malicious program, and we have taken substantial steps to patch the vulnerability and further secure our infrastructure.

You have certain rights when it comes to identity theft and data privacy. Please see the attached Resources Guide to review the resources made available to you. Additionally, we are making available Identity Protection Services available to you free of charge. Please refer to the Resources Guide or contact us at zrent@zrent.net or 781-641-8691 if you are interested.

Sincerely,

ZRent Team
Leader Bank, N.A.
781-641-8691

180 Massachusetts Avenue, Arlington, MA 02474
Phone: 781-646-3900 • Fax: 781-646-3910
www.leaderbank.com

Leader Bank
A STEP AHEAD

Resources Guide

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and other financial information for suspicious activity. In addition, please be aware of the following information:

- If you are a victim of identity theft or fraud, you have the right to file a police report and obtain a copy of it. This notice has not been delayed by law enforcement.

- You may obtain more information about fraud alerts, security freezes and steps you can take to protect against identity theft by contacting the U.S. Federal Trade Commission or your state's attorney general's office, with certain contact information set forth below:
  - Maryland's Office of the Attorney General: 200 Saint Paul Place, Baltimore, MD, 21202; Tel: (410) 576-6300 or visit www.oag.state.md.us
  - US Federal Trade Commission (FTC): The FTC has helpful information about identity theft prevention and other steps that consumer can take to protect themselves.
    - Write to: Consumer Response Center, 600 Pennsylvania Avenue, NW, H-130, Washington, DC, 20580
    - Call Toll-Free: 1-877-IDTHEFT (438-4338)
    - Visit: http://www.ftc.gov/idtheft

- You may obtain a free copy of your credit report once every 12 months and may purchase additional copies of your credit report. Call toll free: 1-877-322-8228; or visit: https//www.annualcreditreport.com; or contact any one or more of the national consumer reporting agencies:
  - Equifax: P.O. Box 740241, Atlanta, GA, 30374; 800-685-1111; www.equifax.com
  - Experian: P.O. Box 2002, Allen, TX, 75013; 888-397-3742; www.experian.com
  - TransUnion: P.O. Box 2000, Chester, PA, 19022; 800-888-4213; www.transunion.com

- You may have the right to place a fraud alert in your file to alert potential creditors that you may be a victim of identity theft. Creditors must then follow certain procedures to protect you; therefore, a fraud alert may delay your ability to obtain credit. An "initial fraud alert" stays in your file for at least 90 days. An "extended" fraud alert stays in your file for 7 years, and will require an *identity theft report* (a filed police report or affidavit filed with the FTC). You may place a fraud alert by calling any one of the three national consumer reporting agencies:
  - Equifax: 800-525-6285
  - Experian: 888-397-3742
  - TransUnion: 800-680-7289

- Certain state laws also allow consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

- If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, the agency cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you a fee based on where you live, which commonly ranges between $3.00 and $15.00, to place, temporarily lift, or permanently remove a security freeze.

Leader Bank
A STEP AHEAD

Resources Guide

- To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:
  - Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348
  - Experian Security Freeze, PO Box 9554, Allen, TX 75013
  - TransUnion Security Freeze, P.O. Box 2000, Chester, PA, 19106

- In order to request a security freeze, you will need to provide the following information:
  - Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
  - Social Security Number;
  - Date of birth;
  - If you have moved in the past five (5) years, provide 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.)
  - If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
  - If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

- The credit reporting agencies 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 in order 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 your 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 your request to remove the security freeze.

- In order to protect yourself against unauthorized activity or identity theft, we recommend that you monitor your credit reports for unexplained or unauthorized activity, and that you monitor all credit cards and other financial accounts in your name for suspicious or unauthorized activity. In order to assist you with these steps, **Leader Bank will provide free credit monitoring services to you through LifeLock Standard identity theft protection**. If you wish to take advantage of these free services, please contact us within fifty (50) days of the date of this letter at 864 Massachusetts Avenue, Arlington, Massachusetts, 02476, or at 781-641-8691, or at zrent@zrent.net.