BY ONLINE SUBMISSION

Maine Office of the Attorney General
109 Sewall St.
August, ME 04330

February 11, 2021

To Whom It May Concern:

On behalf of Citywide Home Loans, LLC ("Citywide" or the "Company"), and pursuant to Me. Stat. tit. 10, §§ 1348, this letter provides notice of a cybersecurity incident affecting five residents of your state. By way of background, Citywide is a licensed mortgage company that provides a range of residential mortgage loan offerings including conventional, FHA, VA and USDA loans.

On November 29, 2020, Citywide experienced a ransomware incident that resulted in the encryption of a number of servers in its data center. Upon discovery, Citywide took a number of its systems offline as a precautionary measure, engaged external cybersecurity experts to assist it in responding to the incident, and reported the incident to law enforcement. The incident did not cause any significant disruption to Citywide's business operations as Citywide's core business systems reside outside of the affected data center and are segmented.

The investigation has determined that, on or about November 18, 2020, an unauthorized third party accessed Citywide's network through the Company's virtual private network ("VPN") gateway using a Citywide employee's username and password for the VPN. The unauthorized party then moved laterally to another location in Citywide's environment and deployed the ransomware, resulting in the encryption of a limited number of Citywide's systems. Citywide has determined that the attackers obtained access to some data on a file share, which is believed to contain personal information associated with some of Citywide's employees and customers, and uploaded this data to Mega, a cloud storage provider.

Upon gaining access to the data at issue, Citywide immediately began working with outside experts to identify all personal information involved to be able to carry out any required notifications pursuant to applicable law. On January 15, 2021, after a detailed search that included a manual review of thousands of files, we determined that the file share contained personal information associated with Citywide customers and employees, including the personal information of five Maine residents. Depending on the individual, the types of information stored on the system may have included the following: name, address, date of birth, phone number, Social Security number, bank account information, and health insurance information. We are not aware of any resulting identity theft, fraud, or financial losses to customers.

Citywide anticipates that it will begin sending these individuals formal notice on or around February 12, 2021 via U.S. mail. A sample of the notification letter is enclosed. As stated in the attached sample notice, Citywide is offering to provide individuals 24 months of free identity theft and credit monitoring services through Kroll. We have also established a call center to respond to individuals' questions.

Citywide, with the assistance of external cybersecurity experts, is taking a number of steps to enhance its security. In response to this incident, Citywide has accelerated a preexisting plan to move all of its technology infrastructure out of its data centers and into the cloud environment of Citywide's parent company. Among other actions, Citywide has also conducted a password reset, strengthened endpoint and Active Directory controls, enhanced its logging and monitoring implementation, and strengthened email filtering controls.

Citywide takes the protection of personal information of all of its customers and employees seriously and is committed to answering any questions that you may have. Please do not hesitate to contact me at (469) 240-2244 or tbergwall@smp.mortgage.

Respectfully yours,

Todd Bergwall
General Counsel

Enclosure

citywide home loans

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

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

<<b2b_text_1(Header)>>

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

<<b2b_text_2(Intro)>> We want to make clear at the outset that keeping personal data safe and secure is very important to us, and we deeply regret that this incident occurred.

WHAT HAPPENED?

On November 29, 2020, we learned that an unauthorized person had gained remote access to Citywide's computer network for a limited period of time and acquired certain information, including personal information<<b2b_text_3(PersonalInfo)>> We took immediate action to contain and remediate the threat, and promptly began investigating the incident. We eliminated the unauthorized access and took further steps to enhance our security.

WHAT INFORMATION WAS INVOLVED?

The information involved may include your name, address, phone number, date of birth, <<b2b_text_4(ImpactedData)>>. We have not identified any evidence that your personal information was used, sold or published by the unauthorized person.

We have seen no evidence that your <<b2b_text_5(ExcludedData)>> was involved in this incident.

WHAT WE ARE DOING

Our security team took prompt steps to address this incident, including contacting law enforcement and engaging third-party cybersecurity experts to assist us in remediating and ensuring the ongoing security of our systems.

We have engaged Kroll to provide two years of identity monitoring services at no cost to you. Your identity monitoring services include Credit Monitoring, Fraud Consultation and Identity Theft Restoration services.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **May 5, 2021** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

WHAT YOU CAN DO

We strongly encourage you to contact Kroll and take advantage of the identity monitoring services we are providing to you free of charge. Remain vigilant and carefully review your accounts for any suspicious activity.

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.

FOR MORE INFORMATION

If you would like to take additional steps to protect your personal information, attached to this letter are helpful tips on how to do so.

We take our responsibility to protect your information extremely seriously, and we are very sorry for any inconvenience that this has caused you. If you have any questions regarding this incident or the services available to you, additional assistance is available by calling 1-855-763-0486 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

<<b2b_text_6(Signatory)>>

Additional Helpful Tips

Helpful Contacts: You can learn more about how to protect your credit by contacting the Federal Trade Commission (FTC) or your state's Attorney General to obtain information including about how to avoid identity theft, place a fraud alert, and place a security freeze on your credit report.

- **Federal Trade Commission,** *Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-IDTHEFT (438-5338), www.ftc.gov/idtheft*

Order Your Free Credit Report. To obtain an annual free copy of your credit reports, visit annualcreditreport.com, call toll-free at 1-877-322-8228, or contact the major credit reporting agencies. Their contact information is as follows:

Equifax:	**Experian:**	**TransUnion:**
equifax.com	**experian.com**	**transunion.com**
freeze.equifax.com	**experian.com/freeze**	**transunion.com/freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-888-909-8872

Fraud Alert: You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit.

Security Freeze: You have the ability to place a security freeze on your credit report at no charge. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent but may delay your ability to obtain credit. To place a security freeze, you must contact each of the three credit bureaus listed above and may be required to provide your full name; SSN; date of birth; the addresses where you have lived over the past five years; proof of current address, such as a utility bill or telephone bill; a copy of a government issued identification card; and if you are the victim of identity theft, the police report, investigative report, or complaint to a law enforcement agency.

Fraud or Identity Theft: If you suspect incidents of identity theft, you should file a report to law enforcement, the FTC, or the Attorney General. If you are the victim of fraud or identity, you have the right to (1) notify the police and Attorney General of your state; and (2) to obtain and file a police report relating to this incident.

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identify theft victims and active duty military personnel have additional rights. For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

State-Specific Notices: Residents of the following states should review the following information:

- **For District of Columbia residents**: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.
- **For Maryland residents**: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.
- **For New York residents**: You may contact the Office of the New York Office of the Attorney General, The Capitol, Albany NY 12224-0341, https://www.ag.ny.gov/, 1-800-771-7755.
- **For North Carolina residents**: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226.

- **For Oregon residents**: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.
- **For Rhode Island residents**: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, http://www.riag.ri.gov/index.php, 1-401-274-4400.
- **For Colorado, Georgia, Maine, Maryland, New Jersey, and Vermont residents**: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional copies.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.