

April 24, 2023

Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202

RE: Data Security Event

Dear Mr. Brown,

loanDepot is submitting this notice to provide your office with information regarding a cybersecurity event that resulted in unauthorized access to consumer personal information ("PI"). loanDepot is a non-bank consumer mortgage loan company based in California.

On August 2, 2022, loanDepot was targeted with a phishing attack that sent malicious emails to 215 employees. The phishing attack leveraged the encrypted email platform Zix, which prevented loanDepot's email security controls from detecting and stopping the malicious emails before they reached the employees. Ultimately, four employees opened the emails and provided their Microsoft Office 365 credentials.

On August 3, the attackers attempted to access the email accounts of the four employees. The initial attempts were unsuccessful because loanDepot had multifactor authentication in place. However, the threat actors subsequently leveraged a legacy authentication protocol to bypass the MFA controls and obtained access to the four accounts. Although loanDepot's security controls prevented connections to its internal network from non-US based IP addresses, the threat actors appear to have used a VPN with US-based egress points that allowed them to connect to the four accounts.

The incident was quickly detected, and resolved within three hours. loanDepot employees became suspicious of the emails and reported them as phishing to the IT department, which immediately launched an investigation. The IT department identified suspicious login activity and issued a company-wide password and session reset, which terminated the threat actors access three hours after the initial intrusion.

loanDepot then retained counsel with cybersecurity expertise and a leading cybersecurity company to investigate the full scope of the incident. The forensic investigation concluded that the incident was limited to the four email inboxes; the threat actors did not access any additional parts of the network, or any data outside of the four email accounts. The investigation did not identify any evidence that the threat actors created mailbox rules, sent personal information from the affected accounts, or moved or deleted data. The investigation indicated, however, that some personal information could have been accessed or acquired by the threat actors during the incident. loanDepot, through counsel, initiated a full manual review of 42,440 documents from the exposed email accounts for the presence of personal information. loanDepot received the results of the document review indicating 1,364 impacted individuals (including 10 in Maryland), their personal information, and their state of residency on April 12, 2023, and determined that it will be notifying certain state regulators. The process of identifying the potentially affected individuals took time to complete due to material personnel changes at loanDepot during the breach response, and because

of the volume and nature of data (including images and handwritten documents) that had to be manually reviewed, formatted, and cataloged.

The following types of personal information were affected:

- Social Security numbers

loanDepot has taken steps to further strengthen its security, including by disabling legacy authentication protocols and moving from approve-or-deny to code-matching MFA. loanDepot has also increased the cadence of its phishing awareness campaigns from quarterly to monthly to better train the workforce to identify and report phishing emails. loanDepot continues to leverage industry-proven solutions to protect its network, data, and customers against cyberattacks.

loanDepot has not observed any evidence that the data has been made public or has been otherwise misused. loanDepot will be notifying any potentially affected individuals and will offer complimentary identity theft protection.

Should you have any questions please do not hesitate to contact our outside counsel: Michael Bahar (MichaelBahar@eversheds-sutherland.com or +1.202.383.0882) or Alexander Sand (AlexanderSand@eversheds-sutherland.com or +1.512.721.2721).

Sincerely,

Joseph Grassi  
Chief Risk Officer  
loanDepot, Inc.



Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

6 1 1358 \*\*\*\*\*SNGLP

SAMPLE A. SAMPLE - All

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



May 5, 2023

Re: Notice of Data Security Event

Dear Sample A. Sample:

At loanDepot, we take privacy very seriously. It is therefore important that we make you aware of data privacy issues that may affect you. Below you will find information about an incident that may have impacted your personal information and the steps we are taking to protect your information.

#### What Happened

On August 3, 2022, we observed anomalous activity on our IT network. We promptly launched an investigation and took a series of immediate steps designed to remediate the issue. loanDepot then engaged a leading cybersecurity firm to further secure our systems, determine the root cause, and further protect your information. loanDepot also reported the event to regulators.

loanDepot identified brief unauthorized access to a small number of internal accounts; this access was terminated and the incident was remediated within three hours. This incident has not affected your loan or our servicing of your account in any way. However, it is possible that the unauthorized actor could have accessed documents containing your personal information, as described below. There is no evidence that any personal data has been misused, but out of an abundance of caution, we wanted to notify anyone that may be affected.

#### What Information Was Involved

Our records indicate that your name and DATA may have been accessed.

#### What We Are Doing

We took a series of immediate steps to remediate the issue, engaged a leading cybersecurity firm to investigate the incident and further protect your information, and we implemented processes and protocols designed to prevent this, or something like this, from happening again.

#### What You Can Do

As discussed further below, we recommend you remain vigilant with respect to reviewing your account statements and credit reports. In addition, to help protect your identity from misuse, we are offering a complimentary 24 month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: August 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

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 (888) 359-0287 by **August 31, 2023**. Be prepared to provide engagement number **B091043** as proof of eligibility for the identity restoration services by Experian.

**Additional details regarding your 24 month Experian IdentityWorks Membership:**

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **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.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 359-0287. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

For More Information

We wanted you to know the nature and extent of this incident and to make you aware of the steps we are taking to protect your information. If you have questions, please call **(888) 359-0287**, Monday through Friday from 9:00 a.m. to 11:00 p.m. and weekends from 11:00 a.m. to 8:00 p.m., Eastern Time. Please have your membership number ready.

Regards,

Joseph Grassi  
Chief Risk Officer  
loanDepot, Inc.

\* Offline members will be eligible to call for additional reports quarterly after enrolling

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

### **Steps You May Take to Protect Yourself Against Potential Misuse of Information**

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also obtain a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

**Equifax:** P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, [www.equifax.com](http://www.equifax.com)  
**Experian:** P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com)  
**TransUnion:** P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, [www.transunion.com](http://www.transunion.com)

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports. We also recommend that you promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

**Federal Trade Commission,** Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

**Fraud Alerts:** There are also two types of fraud alerts that 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 at least 90 days. 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 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed above.

**Credit Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Placing, lifting, and/or removing a credit freeze from your account is completely free and will not affect your credit score. Please contact the three national credit reporting agencies as specified above to find out more information.

The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day, and year); current address and previous addresses for the past 5 years; and any incident report or complaint with a law enforcement

agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state, or military ID card, and a copy of a utility bill, bank, or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit [http://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-underfcra.pdf](http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-underfcra.pdf)

**For residents of New York:** You may also obtain information about security breaches and preventing and avoiding identity theft from the New York Office of the Attorney General: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/>.

**For residents of Massachusetts:** Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**For residents of Oregon:** You may also contact the Oregon Office of the Attorney General: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-877-877-9392, [help@oregonconsumer.gov](mailto:help@oregonconsumer.gov), [www.doj.state.or.us](http://www.doj.state.or.us).

**For residents of Iowa:** You are advised to report any suspected identity theft to law enforcement or to the Office of the Attorney General of Iowa, 1305 E Walnut St, Des Moines, IA 50319, 1-888-373-5044, <https://www.iowaattorneygeneral.gov/>.

**For residents of Maryland:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us).

**For residents of North Carolina:** You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, [www.ncdoj.gov](http://www.ncdoj.gov).

**For residents of the District of Columbia:** You may also contact the District of Columbia Office of the Attorney General: Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, (202) 442-9828, <https://oag.dc.gov/>.