McGuireWoods

McGuireWoods LLP
323 Second St. SE
Suite 700
Charlottesville, VA 22902
Phone: 434.977.2500
Fax: 434.980.2222
www.mcguirewoods.com

Ashley B. Matthews
Direct: 434.977.2570
amatthews@mcguirewoods.com
Fax: 434.980.2250

February 9, 2024

VIA FEDERAL EXPRESS

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Notice of Data Breach

RCVD FEB 12 2024

To Whom it May Concern:

I am writing on behalf of my client, Planet Home Lending, LLC ("Planet"), to report a recent data breach. Planet is a consumer lender located in Connecticut.

Planet was one of many companies around the world whose information security systems were compromised by the threat actor LockBit in connection with one of its recent global ransomware campaigns. The root cause of the incident was a vulnerability (which has been termed "Citrix Bleed") existing in a software program that Planet purchased from Citrix Systems, Inc., a worldwide leader in technology solutions. While Planet had implemented multiple layers of security tools designed to prevent this type of unauthorized access, the threat actor was able to exploit this Citrix Bleed vulnerability to bypass these protections.

The attack occurred on November 15, 2023, and Planet became aware of it that same day. Upon discovery, the company took immediate action to contain the compromise and eradicate the threat. It also retained an experienced outside forensics firm to conduct a thorough investigation into the cause and impact of the breach, to confirm the attack had been contained and no additional unauthorized access had occurred, and to determine whether and to what extent any customer data may have been affected.

On November 28, 2023, Planet was able to determine with reasonable certainty that the threat actor accessed a read-only data folder in which copies of loan files containing personally identifiable information of some of its customers were stored. Once the company was able to make the determination that the data folder had been compromised, it worked diligently to thoroughly analyze the large volume of impacted data in order to determine the specific data elements and parties impacted.

Planet is notifying all consumers whose information was compromised as part of the incident and is offering 24 months of complimentary credit monitoring and identity theft protection through Experian's IdentityWorks. The compromised information includes consumer names, address, Social Security number, loan number, and financial account number.

A draft of the consumer notification letter is attached. As you will see, among other things, the letter describes the remedial measures that Planet took in response to this incident, describes various steps affected individuals can take to protect themselves, and provides information about how the consumer can enroll in complimentary identity and credit monitoring services provided by Experian.

The number of Iowa residents affected by this incident is 2,892.

Thank you for your attention to this notification.

Very truly yours,

/s/ Ashley B. Matthews

Ashley B. Matthews

Enclosure: template notification letter.

185181173_1

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 24, 2024

K7176-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 GENERAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

RE: NOTICE OF DATA BREACH

Dear Sample A. Sample:

Planet Home Lending, LLC ("Planet") is writing to notify you of a recent incident that may affect the privacy of some of your personal information. Planet takes the protection of your information very seriously. Although we have no specific evidence of identity theft or fraud related to your information as a result of this incident, this letter provides information about the incident, our response, and steps you may wish to take to protect against misuse of your information.

What Happened? Planet was one of many companies around the world whose information security systems were compromised by the threat actor LockBit in connection with one of its recent global ransomware campaigns. The root cause of the incident was a vulnerability (which has been termed "Citrix Bleed") existing in a software program that Planet purchased from Citrix Systems, Inc., a worldwide leader in technology solutions. While Planet had implemented multiple layers of security tools designed to prevent this type of unauthorized access, the threat actor was able to exploit this Citrix Bleed vulnerability to bypass these protections.

The attack occurred on November 15, 2023, and Planet became aware of it that same day. Upon discovery, we took immediate action to contain the compromise and eradicate the threat. We also retained an experienced outside forensics firm to conduct a thorough investigation into the cause and impact of the breach, to confirm the attack had been contained and no additional unauthorized access had occurred, and to determine whether and to what extent any customer data may have been affected. On November 28, 2023, Planet was able to determine with reasonable certainty that the threat actor accessed a read-only data folder in which copies of loan files containing personally identifiable information of some of its customers were stored. Once we were able to make the determination that the data folder had been compromised, we worked diligently to thoroughly analyze the large volume of impacted data in order to determine the specific data elements and parties impacted. This notice has not been delayed as a result of a law enforcement investigation.

What Information Was Involved? The investigation determined that certain of your personal information was present in the loan files that were compromised by the threat actor, including the following data elements: name, address, Social Security number, loan number, and financial account number.

What We Are Doing. We take this incident and the security of information in our care seriously. Upon learning of this incident, we promptly secured our environment, conducted a full forensic investigation to determine the nature and scope of the compromise, and notified the FBI. In accordance with the standard recommendation of the FBI and financial regulators, we have not paid, and do not anticipate paying, any ransom amount to the threat actor. We have also implemented additional technical safeguards to help prevent similar incidents in the future. Further, we are currently in the process of retaining a third-party consultant to perform a complete audit and risk assessment of Planet's information security technology, controls and processes, in order to ensure we are employing appropriate safeguards to protect our valued customers' personal information.

Although we are unaware of any actual or attempted identity theft or fraud resulting from this incident, we are offering you access to 24 months of complimentary credit monitoring and identity protection services through Experian's IdentityWorks, which provides you with superior identity detection and resolution of identity theft. Details of this offer and instructions on how to enroll in the services may be found in the attached *Steps You Can Take to Protect Personal Information*. If you would like to enroll in these services, you will need to follow the instructions included on page 3 below, as we are unable to enroll you automatically.

What You Can Do. Please review the information contained in the attached *Steps You Can Take to Help Protect Your Information*. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, monitoring free credit reports you are entitled to receive, and immediately reporting any suspicious activity or incidents of suspected identity theft or fraud to your bank or other financial institution(s). You may also activate your access to the IdentityWorks identity and credit monitoring services we are providing you. There is no charge to you for the cost of these services; however, you will need to follow the instructions on page 3 below to activate your enrollment in this service.

For More Information. If you have questions regarding this incident, you may contact a dedicated assistance line at 833-918-0241 Monday - Friday 9 a.m. to 9 p.m. Eastern Standard Time. You may also write to Planet at 321 Research Parkway, Suite 303, Meriden, CT 06450.

Sincerely,

Planet Home Lending, LLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

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

- Ensure that you **enroll by**: April 30, 2024 (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 833-918-0241 by April 30, 2024. Be prepared to provide engagement number B113012 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 833-918-0241. 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. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** 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 coverage exclusions. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, each consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. We recommend that you periodically obtain a credit report from each nationwide credit reporting agency and request deletion of any information relating to fraudulent transactions. To order a free credit report, visit www.annualcreditreport.com or call toll-free 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free credit report.

You have the right to place an initial or extended "fraud alert" on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a credit file. If a fraud alert is displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. Victims of identity theft are entitled to an extended fraud alert, which is a 7-year fraud alert. If you wish to place a fraud alert, contact any of the three major credit reporting bureaus listed below.

You also have the right to place a free "credit freeze" on your credit report pursuant to 15 U.S.C. § 1681c-1, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your express consent. However, using a credit freeze to control access to the personal and financial information in a credit report may delay, interfere with, or prohibit the timely approval of any request or application made regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze. To request a credit freeze, you may need to provide some or all of the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number or copy of Social Security card;
3. Date of birth;
4. Addresses for the prior two to five years;

5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. If you're a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency.

Should you wish to place a credit freeze or fraud alert, contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
www.equifax.com/personal/credit-report-services/ 1-888-298-0045 Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	www.experian.com/help/ 1-888-397-3742 Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	www.transunion.com/credit-help 1-800-916-8800 TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

In addition to the options outlined above, you may place an alert with ChexSystems. Chex Systems, Inc. is a consumer reporting agency governed by the Fair Credit Reporting Act and other laws. ChexSystems provides account verification services to its financial institution members to aid them in identifying account applicants who may have a history of account mishandling (for example, people whose accounts were overdrawn and then closed by them or their bank). In short, ChexSystems is like the credit reporting agencies (Equifax, Experian, TransUnion) but specific to checking/savings history instead of credit/loan history. ChexSystems offers two protections:

- **Consumer Report Security Alert.** This puts a flag on your consumer file notifying banking institutions that they must take additional steps to confirm the identity of the person initiating the action (much like placing a fraud alert with the credit reporting agencies). You may request a 90-day alert, which is the default, though you may extend it to 7 years if you complete the ChexSystems ID Theft affidavit form (available online), have the affidavit notarized, and send the notarized affidavit to ChexSystems. To set the Consumer Report Security Alert, call (888) 478-6536 or online by visiting www.chexsystems.com.
- **Consumer Report Security Freeze.** This will prohibit ChexSystems from releasing any information in your consumer file without your express authorization, meaning you have to contact ChexSystems and lift the freeze in order for your information to be released (much like placing a freeze with the credit reporting agencies). You should be aware that taking advantage of this right may delay or prevent timely approval from any user of your consumer report that you wish to do business with. The third party will receive a message indicating that you have blocked your information. To set the Consumer Report Security Freeze, call (800) 887-7652 or online by visiting www.chexsystems.com.

Additional Information

You can obtain information from the Federal Trade Commission ("FTC"), credit reporting bureaus listed above, and your state Attorney General regarding identity theft, fraud alerts, and credit freezes, and steps you can take to protect personal information. The FTC may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 877-ID-THEFT (877-438-4338); and TTY: 866-653-4261. The FTC also encourages those who discover that their information has been misused to file a complaint using the FTC's contact information above. You also have the right to file and obtain a copy of your police report if you experience identity theft or fraud. Note that in order to file an identity theft report with law enforcement, you will likely need to provide some proof that you have been a victim. You should also report instances of known/suspected identity theft to local law enforcement and your state Attorney General.

For District of Columbia residents, you may obtain information about steps to avoid identity theft from the FTC and the Office of the Attorney General for the District of Columbia. Contact: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

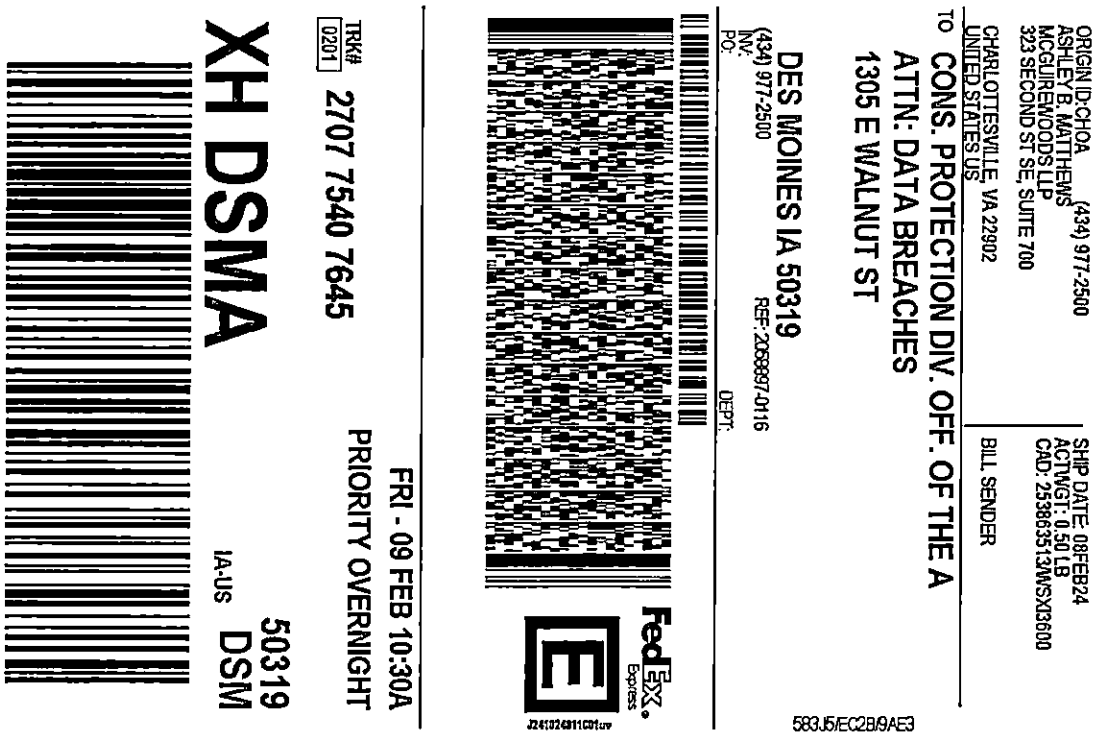
For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, you may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and ncdoj.gov.

For Oregon Residents, the Oregon Division of Financial Regulation (DFR) oversees residential mortgage loan servicers who are responsible for servicing residential mortgage loans in connection with real property located in Oregon and persons required to have a license to service residential mortgage loans in this state. If you have questions regarding your residential mortgage loan, contact your servicer at 866-882-8187 or www.planethomelending.com. To file a complaint about unlawful conduct by an Oregon licensee or a person required to have an Oregon license, call DFR at 888-877-4894 or visit dfr.oregon.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; riag.ri.gov; and 401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event.



FOLD on this line and place in shipping pouch with bar code and delivery address visible

1. Fold the first printed page in half and use as the shipping label.
2. Place the label in a waybill pouch and affix it to your shipment so that the barcode portion of the label can be read and scanned.
3. Keep the second page as a receipt for your records. The receipt contains the terms and conditions of shipping and information useful for tracking your package.

Legal Terms and Conditions

Tendering packages by using this system constitutes your agreement to the service conditions for the transportation of your shipments as found in the applicable FedEx Service Guide, available upon request. FedEx will not be responsible for any claim in excess of the applicable declared value, whether the result of loss, damage, delay, non-delivery, misdelivery, or misinformation, unless you declare a higher value, pay an additional charge, document your actual loss and file a timely claim. Limitations found in the applicable FedEx Service Guide apply. Your right to recover from FedEx for any loss, including intrinsic value of the package, loss of sales, income interest, profit, attorney's fees, costs, and other forms of damage whether direct, incidental, consequential, or special is limited to the greater of 100 USD or the authorized declared value. Recovery cannot exceed actual documented loss. Maximum for items of extraordinary value is 500 USD, e.g. jewelry, precious metals, negotiable instruments and other items listed in our Service Guide. Written claims must be filed within strict time limits, see applicable FedEx Service Guide. FedEx will not be liable for loss or damage to prohibited items in any event or for your acts or omissions, including, without limitation, improper or insufficient packaging, securing, marking or addressing, or the acts or omissions of the recipient or anyone else with an interest in the package. See the applicable FedEx Service Guide for complete terms and conditions. To obtain information regarding how to file a claim or to obtain a Service Guide, please call 1-800-GO-FEDEX (1-800-463-3339).