BUCKLEY

Amanda R. Lawrence
Partner
2001 M Street NW, Suite 500
Washington, DC 20036
t. 202 349-8089
alawrence@buckleyfirm.com

VIA ELECTRONIC SUBMISSION

October 4, 2022

Office of the Maine Attorney General
6 State House Station
Augusta, ME 04333

RE: Aurora Financial Group, Inc. – Notice of Security Incident

Dear Attorney General Frey:

On behalf of Aurora Financial Group, Inc. ("Aurora"), a mortgage master servicer, I write to provide notice regarding a cybersecurity incidents involving Flagstar Bank ("Flagstar") that may have affected the personally identifiable information ("PII") of Aurora's customers. Flagstar, which provides mortgage subservicing, among other services, to Aurora, experienced a cybersecurity incident involving unauthorized access to Flagstar's network that included unauthorized access or acquisition of the PII of certain Aurora's customers (the "Incident"). The written notification from Flagstar related to the Incident is attached.

While Flagstar informed us that it has previously contacted or notified your office and provided appropriate notices to all affected consumers in connection with the Incidents, including the 2 Aurora customers affected by both or either Incident in your state, we are notifying you separately out of abundance of caution. We also are attaching a redacted version of the consumer notice that we understand Flagstar sent to the impacted consumers, which offers 2 years of credit monitoring services from Flagstar.

With respect to the Incident, Flagstar informed us that the potential PII affected included Social Security Number, Account Number/Loan Number, Name, copies of Birth/Marriage Certificates, Credit/Debit Card Numbers, Date of Birth, Digital Signatures, Driver's License or State Issued ID Number, Email Address, Full Access Credentials, Health Insurance Information, Incidental Health References, IRS PIN Numbers, Medicare/ Medicaid Numbers, Military ID Numbers, MRN/Patient IDs, Addresses, Non-U.S. National Identification Numbers, Passport Numbers, Prescription Information, Provider Names, Security Codes and PINs, Security Questions and Answers, Tax ID Numbers, Treatment and Diagnosis Information, and U.S. Alien Registration Numbers.

Upon receiving notice of both the Incident, Aurora began an independent investigation of the Incident, including performing an internal scan of Aurora's network and reviewing access logs which confirmed that no suspicious activity occurred on Aurora's network. Aurora will continue to monitor its systems for suspicious activity. Flagstar also has committed to enhancing its endpoint detection and response tools to prevent future occurrences.

Aurora takes the protection of personal information of all of its customers seriously and is committed to answering any questions that you may have.

Please let us know if you have additional questions or if we can be of further assistance.

Sincerely,

Amanda R. Lawrence

Encl.

September 21, 2022

Wendy Granados
Aurora Financial Group, Inc
Vice President - Servicing Oversight
1451 Route, 34, Suite 303
Farmingdale, NJ 07727

Re: Flagstar Bank, FSB Notification of Data Breach

Flagstar Bank ("Flagstar") is notifying you of a data security incident that involved unauthorized access to our network, and to provide you information about the steps we have taken, and are taking.

What happened?
Flagstar experienced a cyber incident in December that involved unauthorized access to our network. Upon learning of the incident, we promptly activated our incident response plan, engaged external cybersecurity professionals experienced in handling these types of incidents, and reported the matter to federal law enforcement. After an extensive forensic investigation and manual document review, we determined on June 2, 2022, that certain impacted files containing personal information was accessed from our network. We have no evidence that any of the information has been misused.

How will this affect our business operations?
Flagstar has been and remains fully operational. We continue to service our customers as normal. Additionally, to reduce the likelihood of future unauthorized access, we immediately deployed additional detection and response tools across our network for an added layer of security and are taking other measures to harden our cybersecurity defenses. The safety and security of our customer information remains to be our highest priority.

What are our next steps?
On June 17, 2022, we started notifying impacted parties directly via first class U.S. Mail, and have offered them 2 years of complimentary credit monitoring services. We will provide you a list of loans where personal information of the borrower was accessed by the unauthorized third party. We will also provide you copies of the template letters being mailed to our customers who were impacted by this incident.

This notice is provided to ensure full transparency of Flagstar's information security and risk management programs.

Sincerely,

Raj Nukala
Chief Information Security Officer
Flagstar Bank

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Flagstar Bank treats the security and privacy of your personal information with the utmost importance, which is why we are writing to let you know about a recent security incident. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to help protect your information.

What Happened?

Flagstar recently experienced a cyber incident that involved unauthorized access to our network. In response, Flagstar promptly took steps to secure its environment and investigate the incident with the assistance of third-party forensic experts.

What We Are Doing.

Upon learning of the incident, we promptly activated our incident response plan, engaged external cybersecurity professionals experienced in handling these types of incidents, and reported the matter to federal law enforcement. After an extensive forensic investigation and manual document review, we discovered on June 2, 2022 that certain impacted files containing your personal information were accessed and/or acquired from our network between December 3, 2021 and December 4, 2021. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

On June 2, 2022, we determined that one or more of the impacted files contained your <<b2b_text_1(data elements)>><<b2b_text_2(data elements cont.)>>.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Additional information describing your services is included with this letter.

This letter also provides other precautionary measures you can take to help protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Please review the attachment to this letter, entitled “Steps You Can Take to Help Protect Your Information,” for further information. The attachment also includes the toll-free telephone numbers and addresses of the three major credit reporting agencies. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We sincerely apologize for any inconvenience this may have caused you. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at (855) 503-3384. This response line is staffed with professionals familiar with this incident. The response line is available Monday through Friday between 9:00 AM to 6:30 PM Eastern Time, excluding major U.S. holidays.

Visit flagstar.com/protect for further ways you can help protect yourself, including reviewing accounts, checking your credit report and additional best practices to keep your data secure.

Sincerely,

Flagstar Bank
5151 Corporate Drive
Troy, MI 48098

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

- **Activate your Identity Monitoring**
  Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
  You have until ***<<b2b_text_6(activation deadline)>>*** *to activate your identity monitoring services.*
  Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

You've 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'll have the option to call a Kroll fraud specialist, who can help you determine if it's 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 can 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.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements, from us and others, and monitoring your credit reports closely. If you detect any suspicious activity on any account or have reason to believe your information is being misused, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and the Federal Trade Commission ("FTC"). If you file an identity theft report with your local police department, you should ask for and are entitled to receive a copy of the police report. Some creditors may ask for the information contained in the report.

You may be able to obtain information from your state's attorney general on the steps you can take to avoid identity theft. Contact information for your state's attorney general is available at http://www.naag.org/naag/attorneys-general/whos-my-ag.php.

To file a complaint with the FTC, go to https://www.identitytheft.gov/ or call (877) ID-THEFT (877-438-4338), a toll- free number. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies. Additional contact information for the FTC is provided below:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222

For information from the FTC on how federal law limits your liability for unauthorized charges to certain accounts, please visit http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

- **Review a Copy of Your Credit Repo**rt

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every twelve months by visiting https://www.annualcreditreport.com/index.action, calling toll-free (877) 322-8228, or completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action. Or, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies.

Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	*Experian*	*TransUnion*
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. Stolen account information is sometimes held for future use or shared among a group of thieves at different times. Checking your credit report periodically can help you spot problems and address them quickly.

- **Place a Fraud Alert on Your Credit File**

You may want to consider placing a fraud alert on your credit reports. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at https://www.annualcreditreport.com/index.action.

A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may contact any one of the three nationwide credit reporting companies below to place a fraud alert on your files. We recommend that you contact one of the credit reporting companies by phone or online to find out the specific requirements and expedite this process. As soon as one credit reporting company confirms your fraud alert, the others are notified to place fraud alerts. After your fraud alert request, all three credit reporting companies will send you one free credit report for your review.

Equifax
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, PA 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

- **Place a Security Freeze on Your Credit File**

You also have the right to place a security freeze on your credit file. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. To place a security freeze on your credit file, you need to separately contact each of the three nationwide credit reporting companies. A security freeze can be placed on your credit file at no cost to you. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. We recommend that you contact the credit reporting companies, identified above, by phone or online to find out their specific requirements and expedite this process.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
https://www.transunion.com/credit-freeze
(888) 909-8872

- **Best Practices on Helping to Keep Your Data Secure**
  - Do not share personal information over the phone, through the mail, or over the internet unless you initiated the contact or know the person you are dealing with. If someone contacts you unexpectedly and asks for your personal information, even if it is a company you regularly conduct business with, call the company back directly using the published company phone number to verify the request is legitimate before providing any data;
  - Choose PINs and passwords that would be difficult to guess and avoid using easily identifiable information such as your mother's maiden name, birth dates, the last four digits of your Social Security number, or phone numbers. Also, avoid using the same password for online banking that you use for other accounts. Your online banking password should be unique to that account only;
  - Pay attention to billing cycles and account statements and contact us if you don't receive a monthly bill or statement since identity thieves often divert account documentation;
  - Be careful about where and how you conduct financial transactions, for example, don't use an unsecured Wi-Fi network because someone might be able to access the information you are transmitting or viewing.
  - Monitor your accounts regularly for fraudulent transactions. Review payees for online bill payments and Zelle contacts, if applicable. Sign up for account alerts through online banking for certain actions, such as an address or password change. Notify Flagstar Bank immediately if you find any suspicious activity on your account.

- **Research Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit http://www.consumer.ftc.gov/features/feature-0014-identity-theft or call (877) ID-THEFT (877-438-4338).