SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
155 NORTH WACKER DRIVE
CHICAGO, ILLINOIS 60606-1720

TEL: (312) 407-0700
FAX: (312) 407-0411
www.skadden.com

FIRM/AFFILIATE OFFICES
BOSTON
HOUSTON
LOS ANGELES
NEW YORK
PALO ALTO
WASHINGTON, D.C.
WILMINGTON
BEIJING
BRUSSELS
FRANKFURT
HONG KONG
LONDON
MOSCOW
MUNICH
PARIS
SÃO PAULO
SEOUL
SHANGHAI
SINGAPORE
TOKYO
TORONTO

CONFIDENTIAL

March 15, 2021

Via Email SecurityBreach@atg.wa.gov

Office of the Attorney General
1125 Washington St SE
PO Box 40100
Olympia, WA 98504

RE: Flagstar - Accellion Breach

Dear Attorney General:

We write to inform you that Flagstar Bank, FSB ("Flagstar" or "the Company"), 5151 Corporate Drive, Troy, Michigan 48098, will be sending notices to Washington residents advising them of a data breach incident involving Accellion, a vendor that provided a third-party file sharing platform used by Flagstar.

On January 22, 2021, Accellion informed Flagstar that the platform had a vulnerability, which prompted Flagstar to discontinue its use of the platform. Unfortunately, Flagstar subsequently learned on January 24, 2021, that an unauthorized party was able to access some of Flagstar's information on the Accellion platform—and that the Company was one of numerous Accellion clients that were impacted. During its investigation of the breach, Flagstar further learned that the personal information of consumers, including name, address, Social Security Number/tax ID number, date of birth, and/or financial account number without any password or security code that may have provided access to the account, may have been accessed by the unauthorized party. Following a

detailed review of the affected systems, Flagstar determined that 61,006 Washington residents were affected by the incident.[1]

Accellion informed Flagstar that it has reported the matter to law enforcement and Flagstar also notified law enforcement. Following the incident, Flagstar has taken steps to strengthen the security of its systems—such as terminating its use of the Accellion platform involved in the incident and transitioning to another cloud-based product, deploying additional detection and response tools across the Company's network for an added layer of visibility, and taking other measures to harden the Company's cybersecurity defenses—and will take further steps as appropriate to safeguard such information. For the convenience of Washington's impacted residents, Flagstar has arranged to make credit monitoring and identity repair services available to them at no cost for two years.

The formal notice will be sent to the affected residents via first-class U.S. Mail beginning today, March 15, 2021. A copy of the consumer notice template is attached. Please contact me if you have any questions.

Sincerely,

William E. Ridgeway
Counsel to Flagstar Bank, FSB
155 N. Wacker Dr.
Chicago, IL 60606
William.Ridgway@skadden.com

Enclosure

[1] Although Flagstar continues to investigate the incident, the Company wishes to provide notice to the affected individuals as soon as possible. Consequently, this number may not be final. In the event Flagstar identifies additional affected customers in Washington, we will provide a supplemental notice as soon as practicable.

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 >>

Notice of Data Breach

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

Flagstar Bank respects the privacy of your personal information, which is why we are writing to let you know about a recent security incident. Because the privacy and security of the personal information we maintain is of the utmost importance to us, we wanted 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 protect your information.

What Happened?

Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar on January 22, 2021 that the platform had a vulnerability that was exploited by an unauthorized party. Flagstar permanently discontinued use of this file sharing platform. Unfortunately, we have learned that the unauthorized party was able to access some of Flagstar's information on the Accellion platform – and that we are one of numerous Accellion clients who were impacted.

Flagstar remains fully operational and other parts of our IT infrastructure outside of the Accellion platform were not impacted. Importantly, the Accellion platform was segmented from the rest of our network, and our core banking and mortgage systems were not affected.

What We Are Doing.

Upon learning of the vulnerability, Flagstar promptly took the Accellion server offline and permanently discontinued use of this file sharing platform. Additionally, we acted immediately to contain the threat and engaged a team of third-party forensic experts to investigate and determine the full scope of this incident. As part of our investigation, we have also notified law enforcement.

What Information Was Involved?

On March 6, 2021, we determined that one or more of the documents removed from the Accellion platform contained your <<b2b_text_1(DataElements)>>.

What You Can Do.

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 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 Further 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 1-855-907-0446. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday between 9:00 AM to 6:30 PM Eastern Time.

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

Sincerely,

Zahira Gonzalvo, Chief Information Security and Privacy Officer
Flagstar Bank
5151 Corporate Drive ▪ Troy, MI 48098

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

- **Activate Identity Monitoring Services**

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **July 1, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

You've been provided with access to the following services* from Kroll:

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 Report**

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/cra/requestformfinal.pdf. 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	*Experian*	*TransUnion*
(800) 525-6285 www.fraudalerts.equifax.com P. O. Box 105788 Atlanta, GA 30348	(888) 397-3742 www.experian.com/fraud/center P. O. Box 9554 Allen, TX 75013	(800) 680-7289 www.transunion.com/personal credit/ credit disputes/fraud-alerts.page P. O. Box 6790 Fullerton, CA 92834-6790

- **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.

- **Best Practices on Helping to Keep Your Data Secure**

o 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;

o 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;

o 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;

o 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.

o 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).