MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

October 4, 2023

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Supplemental Notice of Security Event

To Whom it May Concern:

We continue to represent Financial Institution Service Corporation ("FISC") located at 500 Pavilion Road, West Monroe, Louisiana 71292. FISC provides data processing and other support services to financial institutions, primarily in Louisiana and surrounding states. We write to supplement our previous notices to your office, which were provided on or about September 22, 2023, and September 28, 2023, regarding the MOVEit Transfer event that may have affected the security of certain personal information relating to New Hampshire residents. This supplemental notice relates to approximately ten (10) additional New Hampshire residents whose information FISC was processing on behalf of certain financial institutions, including: Bank of Abbeville and Trust Company, Citizens Bank and Trust, Citizens National Bank, Franklin State Bank, Citizens Bank & Trust Co. of Vivian, LA, and Basile State Bank. This notice may be further supplemented if significant new facts are learned subsequent to its submission. By providing this notice, FISC does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

As previously reported, on May 31, 2023, and again in June 2023, Progress Software Corporation publicly disclosed a zero-day vulnerability that impacted its MOVEit Transfer software. As a user of that tool, FISC moved quickly to apply available patching, which was first available June 2, 2023, and undertook recommended mitigation steps. FISC promptly launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the potential impact of the vulnerabilities' presence on the MOVEit Transfer server and on the data housed on the server. The

investigation determined that an unknown actor exploited a zero-day vulnerability, accessed the MOVEit Transfer server between May 30, 2023 to May 31, 2023, and exfiltrated certain data from the MOVEit server during that time. FISC subsequently undertook a time-intensive and detailed review of the data stored on the server at the time of the event to understand the contents of that data and to which financial institution that data related. Through this review, FISC determined that certain information related to residents of New Hampshire affiliated with its member financial institutions was present on the server at the time of the event.

FISC's investigation determined the information involved in this event that could have been subject to unauthorized access by the threat actor includes the impacted person's

.

Notice to New Hampshire Residents

On or about June 1, 2023, FISC began to provide preliminary notice of this event to potentially impacted financial institutions while its comprehensive investigation into the event was ongoing. On August 14, 2023, FISC provided impacted financial institutions with formal notice of the event and an offer to provide notification services to potentially affected individuals on their behalf and at their direction. On or about September 22, 2023, and September 28, 2023, FISC began providing written notice of this event to potentially affected individuals on behalf of certain member banks. On October 4, 2023, FISC will continue providing notice to potentially affected individuals, including approximately ten (10) New Hampshire residents who are affiliated with the above-referenced financial institutions on their behalf.

Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of the event, FISC moved quickly to investigate and respond, assess the security of FISC's systems, including its MOVEit Transfer server, and notify potentially affected member financial institutions. FISC also promptly reported the event to federal law enforcement and its primary federal regulators. FISC is providing access to credit monitoring services for 12 months, through Kroll, to individuals affiliated with the impacted financial institutions whose personal information was involved in this event, at no cost to these individuals. FISC also established a toll-free call center for notified individuals affiliated with its impacted financial institutions to address any questions related to this event.

Additionally, FISC is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. FISC is providing individuals with information on how to place fraud alerts and credit freezes on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a

free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

FISC, on behalf of certain impacted financial institutions, is providing written notice of this event to appropriate governmental regulators, as necessary, and to the three nationwide consumer reporting agencies, Equifax, Experian, and TransUnion, all of which were previously notified contemporaneous with the mailing of notification letters to individuals on September 22 and September 28, 2023.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/js

EXHIBIT A

FISC
Financial Institution Service
CORPORATION

<<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(Notice of Data Breach>>

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

Financial Institution Service Corporation ("FISC") provides processing and other support services to financial institutions<<b2b_text_2(, including [data owner])>>. FISC is providing notice of a third-party software event that may affect the security of some of your information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On May 31, 2023 and again in June 2023, Progress Software Corp. publicly disclosed zero-day vulnerabilities that impacted the MOVEit Transfer tool. As a user of that tool, we moved quickly to apply available patching and undertook recommended mitigation steps. We promptly launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the potential impact of the vulnerabilities' presence on the MOVEit Transfer server on the security of data housed on the server. Our investigation determined that an unknown actor exploited vulnerabilities, accessed the MOVEit Transfer server between May 30, 2023 to May 31, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. We subsequently undertook a time-intensive review of the data stored on the server at the time of the event to understand the contents of that data and to whom that data relates. We recently concluded our review.

What Information Was Involved? We determined that the unauthorized access into the MOVEit Transfer server may have rendered accessible information including:

.

What We Are Doing. We take this event and the security of personal information in our care very seriously. Upon learning of this event, we moved quickly to investigate and respond to the event and notify our financial institution partners. As part of our ongoing commitment to the security of information, we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event. We also promptly reported the event to federal law enforcement.

As an added precaution, we are providing you with access to of identity monitoring services provided by Kroll. A description of services and instructions on how to activate can be found within the enclosed *Steps You Can Take to Help Protect Your Information*. Please note that you must complete the activation process yourself, as we are not permitted to activate you in these services on your behalf.

What You Can Do. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, which contains information on what you can do to better protect against possible misuse of your information. We encourage you to remain vigilant against potential incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity for the next twelve to twenty-four months and to report suspected identity theft incidents to your financial institution. You will also find information on how to activate the credit monitoring services offered.

For More Information. If you have additional questions, you may call our toll-free assistance TFN, which is available Monday through Friday, between the hours of 8:00 a.m. and 5:30 p.m. Central time, excluding major U.S. holidays. Also, you can write to FISC at 500 Pavilion Road, West Monroe, Louisiana 71292.

Sincerely,

Financial Institution Service Corporation

Steps You Can Take to Help Protect Your Information

Activate the Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. 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.

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.

Additional information describing your services is included with this letter.

KROLL

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'll 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your 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 copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. You should be aware, however, that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make 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 on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
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. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

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

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

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. To file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; 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 Massachusetts residents, you have the right to obtain any police report filed in regard to this event. 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 New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately [#] Rhode Island residents that may be impacted by this event.