NORTON ROSE FULBRIGHT

April 10, 2023

Norton Rose Fulbright US LLP
1301 Avenue of the Americas
New York, New York 10019-6022
United States of America

Via Certified Mail

Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Tel +1 212 318 3000
Fax +1 212 318 3400

Re: *Legal Notice of Cyber Incident*

Dear Sir or Madam:

I am writing on behalf of my client, Webster Bank, N.A. ("Webster"). Webster's vendor, Guardian Analytics, Inc., a subsidiary of NICE Actimize ("Guardian") was the target of a ransomware attack that affected Webster's data. Based on Webster's investigation, we know that 348 New Hampshire residents were affected, of those 102 New Hampshire residents had their . An additional set of individuals, 246 had , although we believe there is no risk to these individuals, Webster is providing notice to this set of individuals as well.

On January 26, 2023, Webster's Information Security team learned that Guardian suffered a ransomware incident that impacted some of Guardian's systems (the "Incident"). Guardian provides fraud detection services to Webster, as part of those services it processes Webster data.

In response, Webster immediately reached out to Guardian to ascertain more details on the attack. Guardian responded, confirming that an incident had occurred but did not provide further details. On January 27, 2023, Webster's Information Security team identified Webster data on the dark web. On January 29, 2023, Guardian finally notified Webster that its data was impacted (the "Stolen Data") as a result of the incident but did not provide details on the data impacted. In the meantime, Webster began pulling its data down from the dark web to review it. In an abundance of caution, Webster also provided preliminary notice to some regulators, including the Office of the Comptroller of the Currency ("OCC"), Webster's primary federal regulators and the Federal Reserve Board of New York ("FRB NY").

Not until February 10, 2023 did Guardian confirm that Webster's data was impacted and provide access to the Stolen Data for Webster's review. Guardian has only provided minimal cooperation and has provided no meaningful help in reviewing and analyzing the exfiltrated data. Webster, has undertaken this process at its own expense and is providing notification to its individual customers and some commercial customers based on the results of its independent review, which is described below.

According to Guardian, the investigation determined that at least one threat actor (the "Threat Actor") gained access to Guardian's environment on November 27, 2022, via a user's Virtual Private Network (VPN) connection to two (2) domain controllers. During the period of unauthorized access to Guardian's network, the Threat Actor obtained credentials to user accounts and leveraged those accounts to perform network reconnaissance, install remote

access tools, and encrypt systems. The Threat Actor accessed and obtained files and folders at various times between November 27, 2022 and January 17, 2023. On or around January 14, 2023, the Threat Actor exfiltrated data from a non-production environment at Guardian.

Beginning on or around January 20, 2023, two Threat Actors threatened Guardian with the release of the Stolen Data. One Threat Actor, associated with the Daixin ransomware group began posting Stolen Data in late January. Later, around February 10, 2023, the Lockbit ransomware gang began posting Stolen Data. Guardian has not offered an explanation on how two Threat Actors came to possess the Stolen Data. Guardian also confirmed they did not pay a ransom.

With respect to the Stolen Data, it includes . Webster had a team of attorneys and 140 reviewers working to review and identify personal data in the Stolen Data. Beginning on April 10, 2023, Webster will begin notifying individuals who had some combination of , . Webster is notifying and offering all individuals 24-months of complimentary credit monitoring and fraud protection services to them. Webster is extending this offer to all individuals – even if only their name and account number (without a pin or password) was affected.

For our commercial and business banking clients, we are providing them with notice of the incident and, with their permission, we will be notifying any affected individuals associated with those clients. This population is relatively small, but we will provide an update on those notifications if required. We are also working to notify any other financial institutions who may have customers impacted by this incident.

Webster is working with Guardian to ensure that Guardian implements enhanced security measures to safeguard its network, systems, and data, including that of Webster's customers. Webster is also trying to understand why the Stolen Data was stored for this long in a non-production environment. Based on Webster's review, the data appears to date back to 2016. In addition, Guardian confirmed the data was stored in a nonproduction environment, which is prohibited under Webster's contract with Guardian.

Guardian also informed Webster that law enforcement was notified and that Guardian is cooperating with their investigation. In addition, Webster is reviewing its relationship with Guardian going forward.

If you have any questions or need further information regarding this event, please do not hesitate to contact me.

Very truly yours,

David Kessler

WebsterBank

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

April 10, 2023

J2823-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 (LV01 ADULT SSN)
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

RE: Notice of Data Breach

Dear Sample:

We wanted to make you aware of a data security incident that affected Guardian Analytics, Inc. a third-party vendor that provides fraud detection services to Webster Bank. This letter is to provide you with details of what happened, the measures we have taken in response, and to provide you with details on proactive steps you may consider to help protect your information.

What Happened?
On January 26, 2023, Webster learned that Guardian experienced a data security incident that affected a select number of Webster clients. According to Guardian, upon detecting the incident, Guardian immediately activated their incident response plan and retained a third-party cybersecurity firm to conduct an investigation.

Guardian's investigation revealed that unauthorized third parties accessed certain Guardian systems at various times between November 27, 2022 – January 22, 2023. During that time, the unauthorized third parties acquired files that contained Webster clients' personal information from Guardian's systems and later posted the acquired files on the internet.

What Information Was Involved?
Webster reviewed the data that was taken from Guardian's systems and determined that it contained some of your personal information:

What We Are Doing?
Webster has retained third parties to assist with our independent investigation. Additionally, Webster is working with Guardian to ensure they implement enhanced security measures to safeguard their network, systems, and data, including that of Webster's clients. Guardian informed Webster that it has notified law enforcement and is cooperating with their investigation.

What You Can Do?
Please review the "Information About Identity Theft Protection" reference guide (enclosed), which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or security freeze on your credit file.

As an added precaution, to help protect your personal information, Webster Bank is offering a 24-month membership of Experian's® IdentityWorks℠ at no cost to you. This product provides you with identity theft support. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: **July 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:

If you would like additional information including assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **800-910-5176** by July 31, 2023. You will need to provide your engagement number, , as proof of eligibility for the identity restoration services by Experian.

For More Information

If you have any questions or need additional information, please call , toll-free Monday through Friday, between 9 a.m. to 11 p.m. Eastern Time, and Saturday and Sunday from 11 a.m. to 8 p.m. Eastern Time (excluding major U.S. holidays).

The security of your information remains the utmost priority for us. We apologize for the inconvenience and regret that this data incident happened at Guardian.

We value our clients and thank you for doing business with Webster.

Sincerely,

Daniel H. Bley
Chief Risk Officer

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 specialists 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.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.

INFORMATION ABOUT IDENTITY THEFT PROTECTION GUIDE

Free Credit Report. Regardless of whether you choose to take advantage of the complimentary identity monitoring, it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the three nationwide credit reporting companies is as follows

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. You may obtain information from the credit reporting agencies and the FTC about security freezes.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. 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 seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of identity theft and obtaining a police report.
You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.