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

Direct line +1 212 318 3382
david.kessler@nortonrosefulbright.com

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

Office of the Maine Attorney General
109 Sewall St.
Augusta, ME 04330

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 240 Maine residents were affected, of those 82 Maine residents had their name, account number, and SSN affected. An additional set of individuals, 158 residents, had only their name and account number affected, 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 name, financial account numbers (but no pins or passwords), and in some instances, Social Security Number. 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 name, account number and SSN in the Stolen Data. 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