COMMISSIONERS
J.S. Korsmo, Jr.
G. J. Rediske
G. J. Barton

GENERAL MANAGER
Randall M. Black

February 23, 2021

VIA FIRST CLASS MAIL AND EMAIL:

Mr. Bob Ferguson
Washington State Attorney General
1125 Washington Street SE
Olympia, WA 98504-0100
SecurityBreach@atg.wa.gov

RE: AFTS Data Breach Notice

Dear Attorney General Ferguson:

The Lakewood Water District has been made aware of a security/data incident related to its billing vendor, Automatic Funds Transfer Services, Inc (AFTS). The District contracts with AFTS to handle its resident and commercial billing including processing of paper check payments. Please allow this letter to serve as the District's notice pursuant to RCW 42.56.590(7).

The District sent the attached notice to all 14,877 of its customers on February 19, informing them their personal data may have been affected by the breach. At this time, it is unknown whether any District customer data was affected by the breach, as AFTS does not know the full extent of data accessed or taken in the breach. Attached to this letter are the correspondences the District has received from AFTS to date.

The AFTS servers were encrypted by ransomware sometime between the evening of February 3 and the morning of February 4, 2021. The District was made aware of the security/data incident February 11, 2021. There is no direct threat to the District's network as a result of this incident. The District's understanding is that AFTS is working with a cyber security consultant to determine what data was taken. It is also the District's understanding that AFTS refused to pay the ransom demand for the return of the data. The District is no longer using AFTS for its billing needs.

The information of District customers stored in the AFTS databases is limited to data necessary to fulfill billing and payment processing of paper check payments. Breached information from the AFTS database may have included the following personal information: water bill account number, name, address, and billing amounts.

11900 Gravelly Lake Drive SW • Lakewood, WA 98499
Phone (253) 588-4423 • Fax (253) 588-7150

COMMISSIONERS
J.S. Korsmo, Jr.
G. J. Rediske
G. J. Barton
GENERAL MANAGER
Randall M. Black

Additionally, for residents or businesses who paid their utility bills by mailing a paper check, scanned copies of their paper checks are also stored on the AFTS servers which include bank account and routing information. It is unknown at this time whether any personal information of District customers was affected by the breach.

If you have any questions or desire additional information, please contact me at the number below or rblack@lakewoodwater.org.

Sincerely,

Randall M. Black
General Manager

RMB:ckb

Enclosures

cc: District General Counsel Curtis Chambers

11900 Gravelly Lake Drive SW • Lakewood, WA 98499
Phone (253) 588-4423 • Fax (253) 588-7150

LAKEWOOD WATER DISTRICT

COMMISSIONERS
J.S. Korsmo, Jr.
G. J. Rediske
G. J. Barton

GENERAL MANAGER
Randall M. Black

February 17, 2021

Dear Lakewood Water District Customer:

The Lakewood Water District (District) has been made aware of a security/data incident related to its billing vendor, Automatic Funds Transfer Services, Inc (AFTS). The District contracts with AFTS to handle its resident and commercial billing including processing of paper check payments. The AFTS servers were encrypted by ransomware sometime between the evening of February 3 and the morning of February 4, 2021. The District was made aware of the security/data incident February 11, 2021. There is no direct threat to the District's network as a result of this incident.

The information stored in the AFTS databases is limited to data necessary to fulfill billing and payment processing of paper check payments. Electronic payments are processed by a different vendor who is not impacted by the incident. Breached information from the AFTS database may have included your following personal information: water bill account number, name, address, and billing amounts.

Additionally, for residents or businesses who pay their utility bills by mailing a paper check, scanned copies of their paper checks are also stored on the AFTS servers which include bank account and routing information. It is unknown at this time whether these scanned copies of checks have been illicitly extricated from the network. It is also unknown at this time whether any of the District's customer's personal information was extricated from AFTS' network, and if so, what personal information that was. Below are the toll-free telephone numbers and addresses for three major credit reporting agencies in case you want to contact any of them about the AFTS breach:

Equifax—1-800-685-1111; https://www.equifax.com/personal/credit-report-services/; Equifax Information Services LLC, PO Box 740241, Atlanta, GA 30374-0241

Experian—1-888-EXPERIAN (1-888-397-3742; https://www.experian.com/help/; Experian, 475 Anton Blvd., Costa Mesa, CA 92626

Transunion—1-888-909-8872; https://www.transunion.com/credit-help; TransUnion Fraud Victim Assistance, PO Box 2000, Chester, PA 19016

Residents or businesses who pay their water bill by mailing a paper check are encouraged to monitor their bank account for unusual activity and report anything suspicious to their bank right away. **AFTS' databases did not contain social security numbers, birth dates, driver's license numbers, state ID numbers or any other Personally Identifiable Information (PII) of District customers. The breach at AFTS did not impact District customer's credit cards, as AFTS' databases do not contain any personal or commercial business credit card information from District customers**.

The District takes its role of safeguarding personal information very seriously. We continue to discuss additional measures that we can adopt to ensure the highest level of security for personal information. For questions, please contact us at 253-588-4423 or csweb@lakewoodwater.org.

Sincerely,

Randall M. Black
General Manager

RMB:tlm/ckb

11900 Gravelly Lake Drive SW • Lakewood, WA 98499
Phone (253) 588-4423 • Fax (253) 588-7150

AUTOMATIC
FUNDS
TRANSFER
SERVICES

151 S. LANDER, STE. C / SEATTLE, WA 9134

Date: February 9, 2021

To: AFTS Customers

On February 4th, 2021, AFTS servers were the target of a ransomware attack by an overseas malicious actor. Automatic Funds Transfer Services Inc. immediately took our entire network offline and within hours hired a reputable forensic Information Technology company to respond to the ongoing threat of this computer virus. This forensic Information Technology company was tasked with analyzing the extent of the infection of the network virus and determining whether any personal identifying information may have been acquired without authorization.

On February 8th, 2021, Automatic Funds Transfer Services Inc. determined paying the ransom was unreasonable and hired a Seattle based technology company to build a new network while working parallel with the forensic IT company. AFTS upgraded its security systems on this new network and implemented additional security measures.

AFTS has confirmation the malicious actor exfiltrated our network and has some data, but the extent of the data they have is unknown. Depending on the services provided to each customer, the extent of this compromised data may or may not include personal identifying information.

AFTS has reported this event to the FBI and it's been assigned to the Dallas FBI who handles this particular verion of ransomware..

AFTS will be reporting per our requirements to other State and Federal agencies in due course.

Contact Rick Soth by email to: ricks@afts.com if you need additional

From: Christian Fast
To: Curtis Chambers
Cc: Randy Black
Subject: FW: AFTS update
Date: Monday, February 22, 2021 8:13:37 AM
Attachments: LMG_Feb19_00452-2020-001_Status.pdf

Received this update from AFTS over the weekend.
Best regards,
Christian

From: Rick Soth via personal email <ricksoth@gmail.com>
Sent: Saturday, February 20, 2021 1:30 PM
To: Christian Fast <cfast@lakewoodwater.org>
Subject: AFTS update

This message originated outside of the Lakewood Water email system. Please exercise caution opening attachments and links from senders you do not know.

Hello everyone,

We received the attached status report form LMG Security regarding their activities. Not much really new there, but I wanted to pass along what they sent us.

We continue to make progress on getting services back online. Specifically:

- Seattle lockbox services are about 80% restored. We are processing payments for most customers, but continue to be challenged on getting customer A/R posting files generated to make the application of the payments received easier. We are striving to address this since the hand-posting mode many customers are using is a poor substitute.
- Seattle real estate loan servicing is fully operational.
- Our Sacramento and Reno offices are fully operational.
- Our client facing “Portal” that many lockbox clients use is working in general. There are some limitations and challenges being addressed.
- Seattle statement printing and mailing services are still greatly impacted. Progress is being made and we have our formatting systems installed on new server hosts. Our production team are working from new desktop computers as well, and programming is underway to restore our production capabilities as quickly as possible.

We have drilled-into the listing of files the attacker provided to us and have concluded that close to 100% of these filenames are related to our real estate loan servicing business unit. While not great news for the approximate 7,500

accounts we have in this business unit, it is good news for lockbox, statement and other clients and customers that do not appear to be impacted by the exfiltration efforts of the attackers.

We learned Friday from the Dallas FBI agent working our case that once the final report is released from LMG Security, the FBI will be contacting any customers identified in this report to determine the impact this event has had on their business.

This has been a challenging few weeks for everyone at AFTS and our customers. We appreciate our customers loyalty and want everyone to know that we are all working long hours and putting in 100% effort to restore our services. Customer satisfaction with AFTS has historically been very high and we are striving to return to that level as quickly as possible.

Some customers still need to be contacted to discuss their specific issues and needs, and I apologize for the delay in my ability to make those connections, but I hope to get caught up soon.

Rick Soth – ricks@afts.com

(sent via home email address – please do not reply)

Incident Response Status Update

00452-2021-001

AFTS contacted LMG Security for assistance with a ransomware response on February 4, 2021. The ransomware strain has been identified as the .Cuba strain of ransomware. The ransom note indicated that some data was stolen from the AFTS network. The ransomware has been contained, Carbon Black end-point monitoring has been put in place, and recovery and rebuilding is underway.

The requested ransom was $5.6 million. AFTS did not pay the ransom. LMG identified a site on the dark web that claims to have data from AFTS for sale. LMG is in the process of attempting to verify whether or not the data exists and does belong to AFTS.

Further analysis will be on-going to determine access and exfiltration, as well as confirm method of entry.