March 17th, 2021

VIA EMAIL

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington ST SE
PO Box 40100
Olympia, WA 98504
Email: SecurityBreach@atg.wa.gov

Dear Attorney General Ferguson:

Automatic Funds Transfer Services Inc. (AFTS), located at 151 S. Lander St. STE C, Seattle, WA 98134 is writing to inform your Office of an incident which impacted the personal identifying information of some Washington residents.

On February 4th, 2021, AFTS servers were the target of a ransom malware attack by a malicious actor. Automatic Funds Transfer Services Inc. within hours of discovery hired a reputable forensic Information Technology company to immediately contain the ongoing threat of this computer virus. AFTS began receiving notifications of suspicious activity from our Anti-virus applications around 6AM and by 10AM that same day the network was taken off line and the Forensic IT deployed industry leading countermeasures to contain the attack. This forensic Information Technology company has been tasked with analyzing the data logs to determine extent of the spread of the network virus and determine how much 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 base 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 reasonably believes roughly 695 Washington residents had their Names, email addresses, and Bank Account routing information exfiltrated from the compromised network.

On March 18th, 2021 Automatic Funds Transfer Services Inc. has sent out the following letter to those impacted individuals.

Warm Regards,

Jason M. Feldman Esq.,
AFTS Compliance Officer

AUTOMATIC FUNDS TRANSFER SERVICES

March 18, 2021

Notice of Data Security Incident

Account Number:
94 WA

4- 4- 1692
Jason M. Feldman
151 S. Lander St., STE C
Seattle, WA 98134

Dear Jason M. Feldman,

Automatic Funds Transfer Services Inc (AFTS) is writing to inform you of a data security breach that involved your personal information. You have entrusted AFTS with the security of your personal information and we take this responsibility very seriously. It has become apparent our network was accessed by an unauthorized actor. Automatic Funds Transfer Services Inc. wishes to be as transparent as possible with regard to this intrusion incident which has impacted your protected information. The goal of this letter is to provide information about the data security breach as well as steps you can take to protect your information as we move forward in combating these malicious actors.

What happened: On February 4th, 2021, AFTS servers were the target of a ransomware attack by a malicious actor. Automatic Funds Transfer Services Inc. discovered the breach at 4:00AM and immediate took our entire network offline by 10 AM that day. Within 4 hours of discovery AFTS 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 the types of personal identifying information acquired without authorization. A report was filed with the Cyber Crimes Unit of the Federal Bureau of Investigations.

What information was involved: The Name(s), email addresses, and bank account numbers of our Loan Servicing customers who utilize payments through Automated Clearing House (ACH).

What information was NOT involved: Social Security numbers, birthdates, driver's license numbers, state ID numbers, Credit Card information, and mailing addresses was not impacted.

What we are doing: Automatic Funds Transfer Services Inc. discontinued working with the previous network security provider and immediate hired a reputable IT company to build a brand-new network from the ground up. This new network features enhanced security measures designed to reduce the risk of any future incidents.

What steps you can take: AFTS encourages you to remain vigilant by reviewing your personal bank account statements to balance your account and detect errors resulting from any unauthorized activity.

Who do I contact if I have questions?: Please contact Automatic Funds Transfer Services Inc. Compliance Officer Jason Feldman, toll free at 1-800-275-2033 x212, mail: PO Box 34108, Seattle, WA 98124-1108 or at https://www.afts.com.

Sincerely yours,

Eric Johnson

Eric Johnson, President

For more information: AFTS always recommends that you place a fraud alert on your credit file even though it appears no Social Security information was impacted by this data breach. Fraud alerts tell creditors to contact you before they open any new accounts or change your existing accounts. You can call any one of the three major credit bureaus whose information is below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: https://www.equifax.com or 1-800-685-1111, P.O. Box 105069 Atlanta, GA 30348

Experian: https://www.experian.com or 1-888-397-3742, P.O. Box 9554 Allen, TX 75013

TransUnion: https://www.transunion.com or 1-888-909-8872, P.O. Box 2000 Chester, PA 19016

Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

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 reviewing the Credit Bureaus contact information listed above.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order 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.

If your personal information has been misused, visit the FTC's site at https://identitytheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You have rights pursuant to the Fair Credit Reporting Act, such as:

I. the right to be told if information in your credit file has been used against you
II. the right to know what is in your credit file
III. the right to ask for your credit score, and
IV. the right to dispute incomplete or inaccurate information.

Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must:

I. correct or delete inaccurate, incomplete, or unverifiable information;
II. consumer reporting agencies may not report outdated negative information;
III. access to your file is limited; you must give your consent for credit reports to be provided to employers;
IV. you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and
V. you may seek damages from a 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. You can 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.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General listed below.

The Federal Trade Commission	600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261.
Washington State Residents:	Office of the Attorney General,1125 Washington ST SE, PO Box 40100, Olympia, WA 98504, Visit the Washington State Attorney General Identity Theft/Privacy page (www.atg.wa.gov/identity-theftprivacy) for more information. Telephone: 360-753-6200