STATEWIDE
SAFETY SYSTEMS

<<Date>> (Format: Month Day, Year)

<<first_name>> <<last_name>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<last_name>>:

You are receiving this letter in your capacity of your relationship with Statewide Safety System, ("Statewide"). Statewide is the operating name for Statewide Traffic Safety and Signs, Inc, Safety Systems and Signs Hawaii, Inc., Maneri Sign Co., Inc., Altus Traffic Management, LLC, and Traffic Solutions Corporation.

We are writing to inform you about a cybersecurity incident impacting some of your personal information. Promptly after learning of the issues, we took steps to understand its nature and scope and to secure our systems. We engaged leading outside security experts to assist with our investigation and have implemented additional information security measures to enhance our safeguards. We also notified law enforcement of the incident.

What Happened?

Based on our investigation, we learned that a security incident affected certain of your personal information. On April 14, 2021, Statewide discovered it was the victim of a ransomware attack. Statewide immediately took steps to address the issues, including coordinating with leading cybersecurity and forensics experts to investigate and respond to the incident. Our investigation has revealed that cyber criminals were able to acquire certain files from our systems—those files contained personal information about our current and former employees, business contacts, and others. In limited cases, the files contained information about our employees' beneficiaries and dependents. Statewide took immediate efforts to contain and mitigate the cyberattack. We also launched an extensive investigation to determine what personal information was impacted as a result of the incident.

What Information Was Involved?

If you are receiving this letter, Statewide has determined that you are part of the group of individuals whose personal information was impacted. The impacted records contained certain personal information such as name, contact information, date of birth, government-issued ID (such as Social Security number, tax ID, and driver's license, and passport numbers), financial account numbers and medical information. Not all of this information was affected for each impacted individual.

What We Are Doing.

Statewide is committed to ensuring the security of all personal information in its control. As mentioned above, upon discovery of this incident Statewide took immediate steps to contain the incident, conducted a thorough forensic investigation to determine the nature and scope of the incident, and made efforts to mitigate all potential harms. We are alerting you about this incident so you can stake steps to help protect your information.

What You Can Do

Statewide encourages you to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity. Additionally, security experts suggest individuals to contact his/her financial institution and major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on credit files. Statewide also cautions you to never assume an email message requesting that you provide account credentials via a link in an email is legitimate.

As a precautionary measure, Statewide is providing each potentially impacted employee with a complimentary 12-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: <<b2b_text_6(Activation deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: <<ActivationCode (S_N)>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by <<b2b_text_6(Activation deadline)>>. Be prepared to provide engagement number <<b2b_text_1(EngagementNumber)>> as proof of eligibility for the identity restoration services by Experian.

In the meantime, we encourage you to take the following steps to further protect your information:

1. Closely monitor your financial account and promptly contact your financial institution if you notice any unusual activity.
2. Report incidents of suspected identity theft to your local law enforcement, the Federal Trade Commission, and your state attorney general. To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.
3. Take advantage of additional free resources on identity theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

   For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.
4. Monitor your free credit reports. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, by calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.
5. Place a security freeze on your credit files by calling each of the three credit reporting agencies (Equifax, Experian, and TransUnion). Freezing credit files will prevent someone from using your personal information to open new accounts or borrow money in your name. Please understand that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card unless you temporarily or permanently remove the freeze.
6. Contact the three credit reporting agencies to notify them of this incident, receive credit alerts, or freeze your credit filed. Contact information for the three agencies is provided below:

Equifax	Experian	TransUnion
(866) 349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	(888) 397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	(800) 888-4213 www.transunion.com P.O. Box 1000 Chester, PA 19016

For More Information

Statewide is committed to ensuring that the personal information of our current and former employees is protected, and we apologize for the frustration and concern this incident causes. If you have questions, please call our dedicated call center at 1-855-912-1521, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Thank you for your patience and understanding as we work through this process.

Sincerely,

Marty Breen, CFO
Statewide Safety Systems

ADDITIONAL IMPORTANT INFORMATION

More information can also be obtained by contacting the Federal Trade Commission: Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877- IDTHEFT (438-4338); www.identitytheft.gov

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

It is also required by state law that you are informed of your right under the federal Fair Credit Reporting Act (FCRA). The FCRA promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. 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.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. 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 residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877- IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section: 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection: 1300 Broadway, 9th Floor, Denver, CO 80203 1-720- 508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General: 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1- 888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1- 877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov