February 6, 2017

To All US-Based AmTote Employees and US-Based AmTote employees separated from service in 2016:

We are contacting you because we have learned of a recent data security incident that involved certain personal information of our employees. Although we are still investigating this matter, we wanted to alert you of the incident so you can take steps to mitigate the impact.

What Happened?

On Wednesday, February 1, 2017, a file containing 2016 IRS Form W-2 information for all US-based AmTote employees was inadvertently emailed to a third party. We became aware of the incident on February 4, 2017. As a result of this mistake, we believe approximately 350 employee and former employee records were compromised. The compromised information consisted of W-2 information, including employee names, mailing addresses, social security numbers, and salary information.

This does not mean that your identity has been stolen; it means that your W-2 information is now potentially in the hands of a third party.

What Remedial Steps Are We Taking?

Since discovering the incident, we have convened the response team, including outside IT Security Council, to further investigate and respond to this attack, including reviewing methods to prevent similar incidents in the future. Additionally, we are arranging to provide identity theft monitoring and other services for you for a period of one year **at no cost to you**. You will be receiving information regarding this service and how to sign up in the coming days.

What Additional Steps Can You Take?

We strongly encourage you to take additional actions now to help prevent misuse of your information, including the following:

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an

AmTote International, Inc. *11200 Pepper Road* *Hunt Valley, Maryland 21031-1202* *PH: 410-771-8700* *FAX: 410-785-5295*

account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

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.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, 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. You can access the request form at:

https://www.annualcreditreport.com/requestReport/requestForm.action.

Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

- **Credit Report Monitoring/Identity Theft Protection Services**

As mentioned earlier, we are arranging to provide identity theft monitoring and other services for you for a period of one year at no cost to you. You will be receiving information regarding this service and how to sign up in the coming days.

- **Consider Placing a Security Freeze on Your Credit File**

In some states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, cell phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $5 to place, lift, or remove the security freeze.

- **Take Advantage of Additional Free Resources**

You can obtain more information about how to prevent identity theft at www.usa.gov/identity-theft. The theft of personal information can also be used to file fraudulent tax returns. There may be certain actions you can take to help prevent a fraudulent tax return from being filed, including filing a form to notify the IRS that you have been a victim of identity theft. We encourage you to visit www.irs.gov/uac/taxpayer-guide-to-identity-theft for more information.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at:

http://www.marylandattorneygeneral.gov,

or by sending an email to idtheft@oag.statemd.us, or calling 410-576-6491.

Who Can You Contact for More Information?

Because we are still conducting an investigation, we ask that you **NOT** discuss this incident outside of the company other than with family members who have an immediate need to know. Public disclosure of this incident could impede our investigation and could prompt further attacks on the company. Should you have any questions or concerns,

please email idsupport@amtote.com and your questions will be routed to the incident response team.

We sincerely regret this has occurred. Thank you in advance for your understanding and rest assured we are working diligently to combat incidents such as this from happening in the future.