Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

January 12, 2017

By Email: IdTheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of Data Breach

To Whom It May Concern:

I am writing to you on behalf of my client, TrustComm, Inc. ("TrustComm" or the "Company") and pursuant to the Maryland Personal Information Protection Act ("PIPA") Section 14-3504(h) to inform you of a data breach. In the afternoon of January 10, 2017, TrustComm determined that earlier that day, a criminal impersonating a senior Company official had requested and received Internal Revenue Service (IRS) W-2 forms, containing the personal information of a number of employees of the Company, including their Social Security numbers.

The Company promptly reported the incident to law enforcement and is actively cooperating with the authorities in their investigation of this illegal activity.

Pursuant to PIPA, notification is being sent to 4 Maryland residents in substantially the form attached hereto with email and/or mail distribution beginning on or about January 12, 2017. In addition to providing affected individuals with information regarding credit reporting agencies, security freezes, fraud alerts, and other identity theft prevention tools, the Company is also providing all affected individuals with twenty-four (24) months of identity protection services through AllClear ID.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

Allison J. Bender

Senior Associate
allison.bender@hoganlovells.com
D 202.637.5721

Enclosure

January 12, 2017

VIA EMAIL

TrustComm, Inc.
Quantico Corporate Center
800 Corporate Drive, Suite 421
Stafford, VA 22554 USA

[Name of Individual]
[Address]

Re: NOTICE OF DATA BREACH

Dear [Name],

The purpose of his letter is to advise you of an incident that occurred on January 10, 2017 where certain of your personal information was obtained fraudulently by an external source. This letter describes the incident and the actions we have taken and are taking to protect your information.

What Happened

In the afternoon of January 10, 2017, TrustComm, Inc. ("TrustComm" or the "Company") determined that earlier that day, a criminal impersonating a senior Company official had requested and received Internal Revenue Service (IRS) W-2 forms for the year 2015, containing the personal information of a number of employees of the Company, including their Social Security numbers.

What Information Was Involved

Information found in employee W-2 forms, including name; address; wage information; state, local, and federal income tax information; and Social Security number, was involved in this incident.

What We Are Doing

Upon learning of the incident, we promptly contacted law enforcement, and we will cooperate with them to investigate this illegal activity. Privacy and security is a responsibility that we take seriously at TrustComm.

What You Can Do

To help protect you, TrustComm has engaged AllClear ID, Inc. to provide you with identity protection services for twenty-four (24) months at no cost to you. The following identity protection service starts on the date of this notice, and you may use them at any time during the next twenty-four (24) months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will

help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com using the following redemption code: {Redemption_Code}.

Please note: Additional steps may be required by you in order to activate phone alerts and monitoring options.

Even if you choose not to enroll in the services, we recommend that you remain vigilant about your personal information by reviewing account statements you have with other companies and by checking your credit report from one or more of the national credit reporting companies periodically. Following such reviews, you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities.

Because your Social Security number was involved, we recommend that you place a fraud alert on your credit files. You may add a fraud alert to your credit report file to make it more difficult for someone to get credit in your name by requiring creditors to follow certain procedures. It may also delay your ability to obtain credit. To place a fraud alert on your file, contact one of the three nationwide credit reporting agencies; the first agency that processes your fraud alert will notify the others to do so as well. You may also add a security freeze to your credit report file to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

Equifax
800.525.6285
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian
888.397.3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion
800.680.7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. In addition, you may request that the Internal Revenue Service (IRS) mark your account to identify any questionable activity by submitting Form 14039, "Identity Theft Affidavit," for actual or potential identity theft victims. This form is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1.877.IDTHEFT (438.4338), www.ftc.gov/idtheft

Residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1.888.743.0023, www.oag.state.md.us.

For More Information

If you have any questions, please contact Jennifer Maus at [redacted].

Sincerely,

Robert Roe
Chief Executive Officer