Information About a Data Security Incident

TAM International Inc. announced that it has notified some of its current and former employees of an incident involving a ransomware attack. The notice explains what occurred, the information involved, and the measures taken by TAM to investigate and respond to the incident. TAM is not aware of any misuse of any employee information, and it sent notification letters as a precautionary measure. Because current contact information is not available for all former employees, TAM is posting this temporary notice to its website. The substance of the notification letters is set forth below, including steps individuals may consider taking to reduce the risk of identity theft.

What happened?

On or about Saturday, October 24, 2020, cyber criminals encrypted some of TAM's servers and network-connected computers and demanded a ransom to decrypt them. The cyber criminals also claimed that they had stolen files from TAM's servers, targeting certain of TAM's executive team. In response, we retained cybersecurity forensic experts to investigate the incident, restore IT services, and help TAM safely and securely resume operations. The investigation discovered that the attack originated from a company laptop for an employee based outside of the United States. The laptop was compromised via a phishing email in March 2020, and the criminals loaded malware onto the laptop, which later spread to TAM's network. Because of limited available log data, TAM was unable to determine whether the criminals actually acquired, or the extent to which they accessed, sensitive personal information for non-executive employees. Yet because the criminals could have accessed files that contained some of your sensitive personal information, we contacted current and former employees whose information was potentially affected.

What information was involved?

The criminals claimed to have taken copies of certain server files, but our investigation was only able to confirm that the personal data of some of TAM's executives were actually copied. In an abundance of caution, we want you to know that at least one of the network folders that the criminals claimed to have targeted included sensitive personal information of some TAM employees. The files on this network folder contained the following types of sensitive personal information relating to certain current and former employees of TAM: names, addresses, social security numbers, dates of birth, and other personal information.

What we are doing.

TAM moved swiftly to reset passwords to network accounts and implemented additional security controls to prevent further unauthorized access to TAM's network. TAM also notified law enforcement. Since the cyber criminals encrypted TAM's servers, TAM relied on backups to both investigate what information the criminals had potentially accessed and get TAM's operations back online. Yet even TAM's backups carried a risk of reinfection due to the type of malware used. Thus, while the investigation and remediation took additional time, it is complete, and we want to provide this notice to you. We are unaware of any misuse of any employee information at this time.

What you can do.

You should remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitor your credit report for unauthorized activity. You may also consider placing a fraud alert or credit freeze with each of the three credit bureaus. You are also entitled to a free credit report every year from each of these agencies at www.annualcreditreport.com. More information on these and other steps you may take to guard your information and monitor your accounts is included in the "Additional Resources" set forth below.

For more information.

Protecting your information is important to us. If you have questions about whether your information may have been involved in this incident, please call Mike Potter at 713-292-1657 or email him at Mike.Potter@tamintl.com.

ADDITIONAL RESOURCES

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. We recommend periodically obtaining credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus listed below directly to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);

2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-888-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft prevention, 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.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. 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 way of the 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662; 1-888-743-0023; or www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what

is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. 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. We encourage you to 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.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000; or www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Australian residents, the Office of the Australian Information Commissioner publishes information on identity fraud, including how to report fraud, get a copy of your credit report, and apply for a Commonwealth Victims' Certificate to re-establish your credentials and remove fraudulent transactions from the records of business and government agencies, at the following link: https://www.oaic.gov.au/privacy/data-breaches/identity-fraud/. Australian Federal Police also publishes resources at the following link for potential victims of identity crimes, including steps to protect against becoming a victim of identity theft: https://www.afp.gov.au/what-we-do/crime-types/fraud/identity-crime.

For Canadian residents, the Canadian Office of Consumer Affairs publishes information on how to protect your personal information, recognize identity theft and fraud threats, and report identity theft and fraud, at the following link: https://www.ic.gc.ca/eic/site/Oca-bc.nsf/eng/ca03025.html.

For United Kingdom residents, if you think you are a victim of identity theft or fraud, you may contact the Credit Industry Fraud Avoidance System at CIFAS, 6th Floor, Lynton House, 7 - 12 Tavistock Square, London, WC1H 9LT and www.cifas.org.uk. The UK Information Commissioner's Office also publishes information on how to reduce the risk of identity theft and report identity theft: https://ico.org.uk/your-data-matters/identity-theft.