3506 NW 35th
Portland, OR 97210
ph 503.224.7230
fx 503.224.5952
www.metropresort.com

**FOR IMMEDIATE RELEASE**
January 19, 2021

**Media Contact**
Brad Barton, President of Metro Presort, Inc.
bbarton@metropresort.com, 503.224.7230

# Metro Presort Hit by Ransomware Incident; Health Care Clients Notifying Patients and Plan Members

**PORTLAND, Ore. —** Starting this week a number of local health care providers and some health plans are notifying patients and plan members that one of their mail printing and processing service providers, Metro Presort, Inc., suffered a ransomware attack May 6-15, 2019. Those health care clients, along with the number of persons being notified by each, include the following entities, who have joined Metro Presort in issuing this media release:

Oregon Heart Center, PC. – 3,172
Salem Clinic, P.C. – 20,928

Metro Presort is a small family-owned printing and mail processing business that has been in business in Portland for more than 35 years. It processes customer printing and mailing work orders by receiving electronic data files containing addressee information and letter content known as "customer data files" through a secure online portal and temporarily stores and processes these files on company servers.

The ransomware attack on Metro Presort involved malware known as "RYUK," which frequently has been used to attack banks and large health care organizations. The RYUK attack made Metro Presort's computer systems and the data stored on them unusable, including all customer data files, and the criminals that made the attack demanded payment to unlock Metro Presort's systems and information. Metro Presort did not pay the ransom. Metro Presort did not find any evidence indicating that someone without authorization actually accessed any customer data files, but it could not rule out altogether the possibility that the attacker potentially could have had the ability to access such files.

At the time of the ransomware attack, Metro Presort was processing mailings for 21 health care organizations, some of which contained protected health information. These mailings ranged from marketing materials to statements to invoices. Some of the customer data files contained only names and addresses. Other files contained names, addresses, health plan ID numbers, and treatment information. No Social Security numbers, other government ID numbers, or

Metro Presort
3506 NW 35th
Portland, OR 97210
ph 503.224.7230
fx 503.224.5952
www.metropresort.com

financial account information (*e.g.*, credit card or bank accounts) were stored on Metro Presort's systems.

The U.S. Department of Health and Human Services, Office for Civil Rights ("***OCR***"), which enforces the federal health information privacy law known as HIPAA, investigated Metro Presort's response to the incident and its data privacy and security practices. On December 31, 2020, OCR issued a ruling finding no violations of HIPAA and closed its investigation.

The Metro Presort clients that are sending notices to individuals, along with the number of individuals to whom notices will be sent by each client, are listed at the beginning of this announcement. (If additional clients send notifications, this list and notice will be updated.)

"As we've all heard in the news, hackers and malicious computer programs are increasingly targeting all kinds of organizations—from the highest levels of the federal government to local school districts, major companies, large health care organizations, and even cybersecurity firms," said Brad Barton, President of Metro Presort. "It is distressing that there are people in the world deliberately wrecking businesses and trying to profit from others' losses, while also potentially causing problems for individuals. Words cannot express how truly sorry we are about the attack. We take our responsibility to protect and take care of our clients' information very seriously. For several years, we have devoted considerable resources to enhancing our cybersecurity and testing for vulnerabilities, and after the incident we increased our efforts."

***WHAT HAPPENED*.** On May 6, 2019, Metro Presort experienced what initially appeared to be a server outage. Metro Presort later learned that it had suffered a ransomware attack that prevented access to company data, including customer data files. This incident was contained by May 15, 2019, when all affected systems were permanently disconnected, and the threat was neutralized by an advanced endpoint protection solution. Metro Presort did not pay the ransom and never heard further from the attacker or received any indication that the attacker exposed any information on its systems. Metro Presort informed many of its customers of this incident because of ensuing processing delays while it restored data from backup files or obtained second copies of data files from customers. Based on its initial investigation, Metro Presort understood that customer data files were already encrypted on its systems before the incident and that there was, therefore, a low probability of risk to protected health information on client mail data files. Thus, Metro Presort concluded that a reportable breach incident had not occurred and did not provide formal notification to clients.

In September 2020, OCR asked Metro Presort to provide information about this incident. Metro Presort revisited its earlier investigation and findings and determined on October 20, 2020, that it is at least possible that the ransomware attackers could have gained unauthorized access to customer files. Although there were encryption controls available for customer data files, Metro Presort does not have conclusive evidence that customer data files were actually

Metro Presort

3506 NW 35th
Portland, OR 97210
ph 503.224.7230
fx 503.224.5952
www.metropresort.com

encrypted at the time of the incident. The records that would address this issue were lost in the ransomware attack. And although Metro Presort has not uncovered evidence of actual unauthorized access, it cannot demonstrate with absolute certainty that an unauthorized user did not and could not access customer data. Because there was a potential for unauthorized access, Metro Presort is treating this incident as a possible breach.

As noted above, on December 31, 2019, OCR issued a ruling finding no violations of HIPAA and closed its investigation.

***WHAT IS BEING DONE BY METRO PRESORT AND ITS IMPACTED HEALTH CARE CLIENTS.*** Again, Metro Presort takes its obligation to maintain the privacy and security of customer information seriously and has invested substantial resources over the past several years in these areas, including regular security audits, risk assessments, and penetration and vulnerability testing performed by third parties; assigning staff full time to administer network and system security; regular employee training; and working with a managed services provider. Since the incident, Metro Presort has invested additional resources to enhance security, including appointment of an executive within the company to oversee and manage security; engaging a new managed services provider; performing additional risk assessments, security audits, and penetration and vulnerability testing; expanding security training of employees; completely re-evaluating and revising, as needed, its privacy and security policies and procedures; instituting additional security safeguards and controls to minimize the risk of any future incident, including mandatory and verifiable encryption of customer data files at rest and in transit; and working to identify a health care compliance consultant to support our business. Metro Presort notified the Federal Bureau of Investigation about the incident and provided details about the incident and its operations to OCR.

Metro Presort also notified relevant health care clients. Those clients, listed above, then worked with Metro Presort to identify and notify individuals potentially impacted by the possible breach. A toll-free call center was established to answer questions by such individuals: 833-971-3304.

***WHAT INDIVIDUALS CAN DO TO PROTECT THEIR INFORMATION.*** Metro Presort has no evidence of any improper access or use of information, but individuals who may have been affected by the incident, should always be vigilant when receiving and responding to correspondence or inquiries from unknown sources. Affected individuals should regularly monitor their personal accounts and information for any unusual activity. If affected individuals notice any unusual activity, then they should immediately notify their financial institutions (for example, a bank or credit card provider) and healthcare providers. Individuals who receive notices in the mail from their health care providers or plans may call (833) 971-3304 from 9 a.m. to 5 p.m. Pacific Time Monday-Friday, if they have any questions.

3506 NW 35th
Portland, OR 97210
ph 503.224.7230
fx 503.224.5952
www.metropresort.com

In addition, affected individuals should carefully review "Identity Theft Prevention and Protection" section below, which summarizes additional steps that individuals can take to protect their personal information, which includes recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on a credit file. It also includes the contact information for the three major credit reporting agencies and suggestions for obtaining and reviewing credit reports.

***About Metro Presort.*** Metro Presort has provided printing and mail processing services to a wide variety of clients since the mid-1980s and currently employs approximately 40 people in living-wage and middle-class jobs. Metro Presort is an active member of the Greater Portland Postal Customer Council and has been recognized numerous times for its commitment to professional growth and support of those active in the mailing community. It is committed to providing excellent customer services and utilizing technology to increase efficiency and client-service value.

MetroPresort

3506 NW 35th
Portland, OR 97210
ph 503.224.7230
fx 503.224.5952
www.metropresort.com

**IDENTITY THEFT PREVENTION AND PROTECTION**

***Monitor Your Accounts and Credit Reports, and Notify Police and the FTC of Suspicious Activity:***
When you receive account statements, credit reports, and monitoring alerts, review them carefully for unauthorized activity. Look for accounts you did not open, unauthorized purchases, inquiries from creditors that you did not initiate, and personal information that you do not recognize, such as a home address or Social Security number. If you have concerns, call your bank, the account provider, or the credit reporting agency. If possible, place a security verification secret word, similar to a password, on your accounts. If you suspect any fraudulent activity or identity theft, promptly report it to local law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. To file a complaint with the FTC, go to https://www.consumer.ftc.gov/features/feature-0014-identity-theft or call 1-877-ID-THEFT (877-438-4338). Request copies of any police or investigation reports created, as you might need to provide this information to credit reporting agencies or to supposed creditors to clear up your records.

***Obtain Free Credit Reports*:** Even if you do not find any signs of fraud on your reports, you should check your credit report regularly. There are three main credit reporting agencies: Equifax, Experian, and TransUnion. Their contact information, along with contact information for the FTC and some state agencies, are on the reverse side. Each credit reporting agency must provide you annually with a free credit report, at your request made to a single, centralized source for the reports, AnnualCreditReport.com. You are not required to order all three reports at the same time; instead, you may rotate your requests so that you can review your credit report on a regular basis. In addition, many states have laws that require the credit reporting agencies to provide you with a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

***Free Services by Credit Reporting Agencies*:** Each credit reporting agency offers additional free services to help you protect your credit. TransUnion at www.transunion.com permits you to sign up for TrueIdentity which is a service that allows you to examine your TransUnion credit file and place a "credit lock" which prevents others from opening up credit in your name. Experian at www.experian.com provides you with a free credit report every month when you select "Start with your free Experian Credit Report." Equifax at www.equifax.com permits you to sign up for "Lock & Alert" which also allows you to place a credit lock.

***Fraud Alert*:** You may ask the credit reporting agencies to place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three credit reporting agencies. As soon as that agency processes your fraud alert, it is supposed to notify the other two, which then also must place fraud alerts in your file. An *initial fraud alert* stays in your file for at least 90 days. An *extended alert* stays in your file for seven years. To place either of these alerts, a credit reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency.

***Security Freeze:*** You also have the right to place a security freeze on your credit report at any of the three main credit reporting agencies. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request. If you choose to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail, the following information must be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency. The request must also include a copy of a

government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and displays your name, current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the agency. The main three credit reporting agencies provide details about their security freeze services and state requirements at the following links:

- Experian: http://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/
- Equifax: https://help.equifax.com/app/answers/detail/a_id/75/~/security-freeze-fees-and-requirements
- TransUnion: https://www.transunion.com/credit-freeze/place-credit-freeze

***Internal Revenue Service*:** Tax-related identity theft is when someone uses your Social Security number to file a false tax return claiming a fraudulent refund. If you received IRS correspondence indicating you may be a victim of tax-related identity theft or your e-file tax return was rejected as a duplicate, do the following:

- Submit an IRS Form 14039, Identity Theft Affidavit, to the IRS;
- Continue to file your tax return, even if you must do so by paper, and attach the Form 14039; and
- Watch for any follow-up correspondence from the IRS and respond quickly.

The fillable IRS Form 14039 is available at IRS.gov. Follow the instructions exactly. You can fax or mail it or submit it with your paper tax return if you have been prevented from filing because someone else has already filed a return using your SSN. You only need to file it once. Do not respond to threats made over the phone or via email that the IRS will take action against you. The IRS will communicate with you in writing.

***Financial Accounts, Oral Passwords and 2FA*:** If financial accounts are affected, contact the institution and ask them about steps you may take to further protect your account. Financial institutions will often permit you to place an oral password on your account or enable multifactor authentication to your online account.

***Contact Information for the FTC, Credit Reporting Agencies, and State Consumer Protection Agencies*:** If you suspect fraudulent activity on any of your financial accounts (savings, checking, credit card) or identity theft, you are encouraged to report your concerns to your financial institutions and the relevant agencies below.

**Federal Trade Commission**
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft/

**AnnualCreditReport.com**
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
www.annualcreditreport.com

**Equifax**
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

**Experian**
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

**TransUnion**
P.O. Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com