



**CJ Elmwood Partners LP**

an affiliate of Jones Eye Clinic

## **NOTICE REGARDING SECURITY INCIDENT**

On August 23, 2018, Jones Eye Center, P.C. ("Jones Eye Clinic") and CJ Elmwood Partners, L.P., the affiliated surgery center of Jones Eye Clinic ("Surgery Center"), discovered a cybersecurity incident involving the personal information of Jones Eye Clinic and Surgery Center patients. Jones Eye Clinic and Surgery Center use a common computer network for patient billing and scheduling. Affected individuals include patients of Jones Eye Clinic and patients of the Surgery Center who were registered or had services at either entity between January 1, 2003 and August 23, 2018.

On the morning of August 23, 2018, we discovered that our computer network suffered a cyberattack called ransomware, a type of computer virus that locks up, or encrypts, information and demands a payment be made in order to unlock the information. That same day, we restored our system using backup information and ended the attack without paying the ransom amount. However, while our systems were under attack, there is the possibility that the attackers could have gained unauthorized access to protected health information of patients of both Jones Eye Clinic and the Surgery Center. We immediately began an investigation, hired a forensic computer investigator, and notified the FBI.

The investigation found that a ransomware virus was loaded on our system one day earlier, on the evening of August 22, 2018. Our experts' review indicated that, during the overnight hours, the attackers would have had the ability to access patient information contained in our patient billing and scheduling software. The attack did not impact our electronic medical records. While unauthorized access to patients' billing and scheduling information might have occurred, we have not received any indication that the information has been misused. According to computer experts and law enforcement, these types of attacks are usually financially motivated and not focused on obtaining patient information. However, because there is a possibility that the information could have been accessed, we are notifying all impacted individuals of this incident.

Information contained in our billing and scheduling software included full name, address, date of birth, date of service, medical record number, and a general description of the clinic visit or surgery. For some individuals, information may have included Social Security number, insurance status, and claims information. The information did not include other financial information such as bank account or credit card information.

After discovering this incident, we engaged multiple information technology companies to assist with restoring our systems and deploying new technology to prevent future intrusions. Although we have found no evidence that patients' information was actually viewed or misused, we encourage affected individuals to take the precautionary measures described below to help protect against identity theft or fraud.

We sent letters to all impacted individuals for whom Jones Eye Clinic and Surgery Center has valid addresses by U.S. mail. The letters contain important information about steps individuals can take to prevent identity theft or fraud.

Affected individuals are eligible to enroll in free credit monitoring services for one year. Instructions on how to enroll are included in the notification letters mailed to affected individuals' last known address.

Below is information about other precautionary measures affected individuals can take, including placing a fraud alert and/or security freeze on credit files and obtaining a free credit report.

For individuals who have questions or concerns about this incident we have established a confidential, toll-free hotline with a dedicated call center (Epiq) that is staffed with professionals familiar with this incident who can assist you with questions and steps you can take to protect yourself against identity theft and fraud. **The hotline is available at 1-877-299-1557, Monday through Friday, from 8 am – 8 pm Central Standard Time.**

Jones Eye Clinic and the Surgery Center take the privacy and security of our patients' information very seriously and we deeply regret an inconvenience this attack may have caused our patients and their families.

#### **- ADDITIONAL PRIVACY SAFEGUARDS INFORMATION -**

##### **Fraud Alert Information**

Whether or not you enroll in credit monitoring, we recommend that you place a "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
<a href="http://www.equifax.com">www.equifax.com</a>	<a href="http://www.transunion.com/fraud">www.transunion.com/fraud</a>	<a href="http://www.experian.com">www.experian.com</a>
1-800-525-6285	1-800-680-7289	1-888-397-3742

##### **Free Credit Report Information**

Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at [www.annualcreditreport.com](http://www.annualcreditreport.com).

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at [www.identitytheft.gov](http://www.identitytheft.gov) or at 1-877-ID-THEFT (1-877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC's website at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) to review their free identity theft resources such as their comprehensive step-by-step guide "Identity Theft - A Recovery Plan".

## Security Freeze Information

You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze  
PO Box 105788  
Atlanta, GA 30348  
<https://www.freeze.equifax.com>  
1-800-685-1111

TransUnion Security Freeze  
PO Box 2000  
Chester, PA 19016  
<http://transunion.com/freeze>  
1-888-909-8872

Experian Security Freeze  
PO Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
1-888-397-3742

- Your full name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.) Your Social Security Number
- Your date of birth (month, day and year)
- Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
- If you have moved in the past 2 years, give your previous addresses where you have lived for the past 2 years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- Include applicable fee. Call or visit each of the credit reporting company websites listed above for information on fees for Security Freeze services. Forms of payment are check, money order, or credit card (American Express, Discover, MasterCard and Visa), or a copy of a valid identity theft report, or other

valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

Within 5 business days of receiving your request for a security freeze, the consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if you choose to remove the freeze on your consumer credit report or to authorize the release of your consumer credit report to a specific party or for a specified period of time after the freeze is in place.

DOCS/2140072.2