

July 28, 2021

**Michael E. Kar, Esq.**  
212.915.5535 (direct)  
Michael.Kar@WilsonElser.com

Via First-Class Mail

Washington State Office of the Attorney General  
800 5th Ave. Suite 2000  
Seattle, WA. 98104-3188

**Re: Our Client : Osborn Cancer Care**  
**Matter : February 2021 Data Security Incident**  
**Wilson Elser File # : 16516.01339**

---

Dear Attorney General Ferguson:

We represent Osborn Cancer Care (“OCC”), with a mailing address of 1201 Bishop Road, Chehalis, Washington 98532, with respect to a data security incident described in more detail below. OCC takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of Washington residents being notified, the name and address of the entity that experienced the breach, what information has been compromised, and the steps that OCC is taking to secure the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impact individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On February 17, 2021, OCC was informed that scans of certain patients' information had been compromised by an unauthorized cybercriminal. OCC contacted its electronic medical record (EMR) provider, GeniusDoc, Inc., and immediately commenced an investigation into the incident. GeniusDoc has confirmed that on February 10, 2021, a cybercriminal infiltrated a portion of GeniusDoc's network environment, resulting in unauthorized access to this personal information.

Following the completion of the investigation, OCC arranged for notification of all individuals whose information is hosted by GeniusDoc, even if their personal information was not located in the compromised network location. Accordingly, OCC is notifying all potentially impacted individuals that their full name, mailing address, driver's license, date of birth, and medical information could have been compromised by this unauthorized party.

As of this writing, OCC has not received any reports of related identity theft since the date the incident was discovered (February 17, 2021 to present).

---

150 East 42nd Street • New York, NY 10017 • p 212.490.3000 • f 212.490.3038

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky  
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix • San Diego  
San Francisco • Sarasota • Stamford • Virginia • Washington, DC • West Palm Beach • White Plains

[wilsonelser.com](http://wilsonelser.com)

## 2. Number of Washington Residents Affected

A total of 4,305 residents of Washington were potentially affected by this security incident. Notification letters to these individuals were mailed on July 26, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

## 3. Steps Taken

Upon detecting this incident, OCC moved quickly to initiate their incident response, which included conducting an investigation with the assistance of third-party forensic specialists and confirming the security of their network environment. OCC has reviewed and altered their tools, policies, and procedures relating to the security of their systems and servers, as well as their information life cycle management. OCC notified the Department of Health and Human Services on June 8, 2021.

OCC is transitioning to a new EMR vendor.

OCC values the safety of their customer's personal information and are therefore offering credit monitoring and identity theft protection services to through IDX.

## 4. Contact Information

OCC remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Michael.Kar@WilsonElser.com or 212.915.5535.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Michael E. Kar, Esq.  
MEK/are

Copy: Robert Walker, Esq. (Wilson Elser LLP)  
Adam Eisler, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*



P.O. Box 989728  
West Sacramento, CA 95798-9728

To Enroll, Please Call:  
1-833-325-1763  
Or Visit:  
<https://app.idx.us/account-creation/protect>  
Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

**Via First-Class Mail**

July 26, 2021

Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

Osborn Cancer Care (“OCC”) is an oncology and hematology specialist with two locations in Washington. We are writing in order to inform you of an incident that may have exposed your sensitive personal and health information. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

On February 17, 2021, OCC was informed that scans of certain patients’ information had been compromised by an unauthorized cybercriminal. OCC contacted its electronic medical record (EMR) provider, GeniusDoc, Inc., and immediately commenced an investigation into the incident. GeniusDoc has confirmed that on February 10, 2021, a cybercriminal infiltrated a portion of GeniusDoc’s network environment, resulting in unauthorized access to this personal information.

Following the completion of the investigation, OCC arranged for notification of all individuals whose information is hosted by GeniusDoc, even if their personal information was not located in the compromised network location. Accordingly, this letter serves to notify you that your full name, mailing address, driver’s license, date of birth, and medical information could have been compromised by this unauthorized party.

As of this writing, OCC has not received any reports of related identity theft since the date the incident was discovered (February 17, 2021 to present).

What We Are Doing:

We value the safety of your personal information and are therefore offering credit monitoring and identity theft protection services through IDX, a leading identity protection technology company. IDX’s services include: <<Variable Data1>> months of credit monitoring and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-325-1763 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX

representatives are available Monday through Friday, 6 am – 6 pm Pacific Time. Please note the deadline to enroll is October 26, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal health information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call IDX at 1-833-325-1763, Monday through Friday, 6 am – 6 pm Pacific Time.

OCC values the security of the personal data that we protect, and we apologize for any inconvenience that this incident has caused.

Sincerely,

A handwritten signature in cursive script that reads "Dustan Osborn".

Dustan Osborn, MD, PhD  
Principal

## Additional Information

**Credit Reports:** You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**Security Freeze:** You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (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 or the Registry of Motor Vehicles. 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

<b>Equifax Security Freeze</b> P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 <a href="https://www.equifax.com/personal/credit-report-services/credit-freeze/">https://www.equifax.com/personal/credit-report-services/credit-freeze/</a>	<b>Experian Security Freeze</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>	<b>TransUnion Security Freeze</b> P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>
---	---	--

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf));
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are listed above.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**File Police Report:** You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**FTC and Attorneys General:** You can further educate yourself regarding identity theft, 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](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338), 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. 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, 1-888-743-0023, and [www.oag.state.md.us](http://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-fera.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fera.pdf) or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and [www.ncdoj.gov](http://www.ncdoj.gov).

**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, and <https://ag.ny.gov/>.

**For Rhode Island residents**, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.