WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

October 4, 2022

Rachel Cobble Pitts, Esq.
205.709.8991 (direct)
Rachel.Pitts@WilsonElser.com

Via electronic-mail: SecurityBreach@atg.wa.gov

Attorney General Bob Ferguson
Office of the Attorney General
800 5th Avenue
Seattle, WA 98104

Re:	**Our Client**	**:**	**Whitworth University**
	Matter	**:**	**Data Security Incident**
	Wilson Elser File #	**:**	**16516.01917**

Dear Attorney General Ferguson:

We represent Whitworth University ("Whitworth"), located in Spokane, Washington, with respect to a data security incident described in more detail below. Whitworth 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 incident, the number of Washington residents being notified, what information has been compromised, and the steps that Whitworth is taking to secure the integrity of its systems. We have also enclosed hereto a sample of notifications being made to the potentially impact individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On July 29, 2022, Whitworth was the target of a ransomware attack. Multiple unauthorized actors infiltrated our network. Upon detecting this incident, Whitworth moved quickly to initiate a response, which included engaging a team of external forensic and cybersecurity experts to analyze the environment and conducting a comprehensive investigation into the sensitivity of data accessed. Whitworth identified individual information was potentially compromised on September 6, 2022, and the list of individuals to notify was finalized on September 12, 2022.

This incident may have resulted in the exposure of employee and student personal information that was located on our systems, including names, student identification number, state identification number, passport number, Social Security number and/or health insurance information could have been exposed as a result of this attack. This information was maintained either by individual departments/employees or for standard administrative purposes.

Whitworth is not aware of any evidence that information has been misused and has not received any reports of related identity theft since the date of the incident.

2. Number of Washington Residents Affected

A total of five thousand, one hundred and eighty two (5,182) residents of Washington have been identified as potentially affected by this security incident. Notification letters to these individuals were mailed on October 3, 2022, by first class mail. Sample copies of the notification letters are included with this letter.

3. Steps Taken

Upon learning of this incident, Whitworth moved quickly to institute a response plan, which included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to confirm the security of any relevant systems. Whitworth wiped and rebuilt affected systems and is taking additional steps to enhance technical safeguards relating to the security of its systems and servers to protect against a future incident. Law enforcement has also been notified.

Although Whitworth is not aware of any evidence of misuse of personal information, Whitworth extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service includes credit monitoring, along with a fully managed identification theft recovery service, should the need arise. Notification letters and offers of free credit monitoring were mailed October 3, 2022.

4. Contact Information

Whitworth 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 Rachel.Pitts@WilsonElser.com or 205.709.8991.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Rachel Cobble Pitts, Esq.

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

Enclosure: *Sample Notification Letters*

WHITWORTH UNIVERSITY

Return Mail to IDX
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-875-0646
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

Via First-Class Mail

October 3, 2022

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

You are receiving this letter because you are a current or former employee of Whitworth University in Spokane, Washington. We are writing to inform you of an incident that may have exposed your personal information. Whitworth University takes the privacy of personal information seriously and wants to provide you with information and resources you can use to protect your information.

What Happened and What Information Was Involved:

On July 29, 2022, we detected and stopped a ransomware attack in which an unauthorized third party accessed and disabled some of our systems. We immediately engaged third-party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity. Our investigation determined an unauthorized third party may have accessed certain individual personal information during this incident.

Our ERP Solution, where the vast majority of employee information is securely maintained, was **not** impacted by the breach. However, some working files stored by departments or individuals on the network share drives were potentially impacted. We found no evidence that your information has been specifically misused; however, it is possible that the following personal information could have been accessed by an unauthorized third party: first and last name, Social Security number, state identification number, passport number, health insurance information.

Again, to date, we have not received information of a specific misuse of personal information. We have taken all efforts possible to mitigate any further exposure of your personal information and related identity theft.

What We Are Doing:

Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of our network environment. We notified law enforcement. We wiped and rebuilt affected systems and have taken steps to bolster our network security. We are also reviewing and altering our policies, procedures, and network security software relating to the security of our systems and servers, as well as how we store and manage data.

We are offering free credit monitoring and identity theft protection services through IDX, a leading identity protection technology company. IDX services include: <<12/24>> months of credit monitoring and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to https://app.idx.us/account-creation/protect and follow the instructions provided. When prompted please provide the unique code found above to receive services. IDX is available Monday through Friday, 6:00 am – 6:00 pm PST. Please note the deadline to enroll is **January 3, 2023**.

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 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 1-833-875-0646, Monday through Friday, 6:00 am – 6:00 pm PST.

We value the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

The Management Team of Whitworth University

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, 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:

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

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);
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 at 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, 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.

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 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.

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, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

WHITWORTH UNIVERSITY

Return Mail to IDX
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-875-0646
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

Via First-Class Mail

October 3, 2022

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

You are receiving this letter because you are a current or former student of Whitworth University in Spokane, Washington. We are writing to inform you of an incident that may have exposed your personal information. Whitworth University takes the privacy of personal information seriously and wants to provide you with information and resources you can use to protect your information.

What Happened and What Information Was Involved:

On July 29, 2022, we detected and stopped a ransomware attack in which an unauthorized third party accessed and disabled some of our systems. We immediately engaged third-party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity. Our investigation determined an unauthorized third party may have accessed certain individual personal information during this incident.

We found no evidence that your information has been specifically misused; however, it is possible that the following personal information could have been accessed by an unauthorized third party: first and last name, Social Security number, student identification number, date of birth, passport number, health information. This information is maintained for standard administrative purposes.

Again, to date, we have not received information of a specific misuse of personal information. We have taken all efforts possible to mitigate any further exposure of your personal information and related identity theft.

What We Are Doing:

Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of our network environment. We notified law enforcement. We wiped and rebuilt affected systems and have taken steps to bolster our network security. We are also reviewing and altering our policies, procedures, and network security software relating to the security of our systems and servers, as well as how we store and manage data.

We are offering free credit monitoring and identity theft protection services through IDX, a leading identity protection technology company. IDX services include: <<12/24>> months of credit monitoring and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to https://app.idx.us/account-creation/protect and follow the instructions provided. When prompted please provide the unique code found above to receive services. IDX is available Monday through Friday, 6:00 am – 6:00 pm PST. Please note the deadline to enroll is **January 3, 2023**.

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 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 1-833-875-0646, Monday through Friday, 6:00 am – 6:00 pm PST.

We value the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

The Management Team of Whitworth University

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, 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:

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

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);
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 at 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, 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.

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 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.

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, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.