



**Human Resources
and Legal Affairs**

12401 SE 320th St.
Auburn, WA 98092-3622

(253) 833-9111 Ext. 3320
(253) 288-3393 Fax

greenriver.edu

24 August 2017

Washington Attorney General's Office
Sent Via Email Only
SecurityBreach@atg.wa.gov

RE: Notification of Security Breach at Green River College

To Whom It May Concern:

This letter will inform you of a recently discovered security breach incident at Green River College (GRC). We discovered on 15 August 2017 that GRC employee personal information was compromised. We believe the data breach occurred sometime in December 2016. The compromised information includes employee names and Social Security numbers. We have taken immediate steps to ensure that employee information held by GRC is now secure, and we are in the process of reviewing the incident to prevent a recurrence of the problem. We are also working with law enforcement to address the security breach.

This security breach involved information on approximately 3399 employees. Employees with compromised information were provided email notice of the breach on 24 August 2017 and a duplicate notice will be sent to the bulk of employees (whose data was readily available) by regular mail on 24 August 2017 but not later than 28 August 2017 for those whose data required additional research. A sample copy of the notice sent to employees is attached.

If you have questions or need addition information about this incident, please contact Marshall Sampson, Vice President of Human Resources & Legal Affairs at 253.288.3315 or msampson@greenriver.edu.

Sincerely,

Marshall Sampson
Vice President of Human Resources & Legal Affairs
Green River College

[Name]
[Address]
[City, State Zip]

24 August 2017

Notice of Data Breach

What Happened

On Tuesday, 15 August 2017, the college learned of a data breach involving employee information. A spreadsheet was downloaded from a campus employee computer on 06 December 2016 to a thumbdrive. At some point, the thumbdrive was mislaid and returned to Campus Safety. Through a regular audit of unclaimed thumbdrives, Safety became aware of the data breach on 15 August 2017.

What Information Was Involved

Information on the spreadsheet was routine in nature. While it included publicly available data (name, salary, department, etc.), **it also included social security numbers**. It did not include date of birth or home address.

What We Are Doing / Have Done

- Per Green River College protocol, appropriate state agencies were notified.
- The Auburn Police were alerted to the situation and informed the college yesterday (Wednesday, 24 August 2017) that they deem this “suspicious circumstances” but not a crime as there is no evidence that the information has been used. Because the appropriate investigation by law enforcement is now complete, the college is communicating with the campus community and impacted individuals.
- While waiting for clearance from law enforcement, the college worked with other state agencies to secure a contract for identity theft protection services.
- A campus forum will take place on Tuesday, 29 August from 1 p.m. to 2 p.m. in Cedar Hall, Room 214.
- In addition, the college will be undergoing an audit of access to information and examining our current practices to ensure that we remain diligent in the protection of data.
- Lastly, you can visit www.greenriver.edu/credit as the centralized location for information as it becomes available.

What You Can Do

Due to this incident, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare. With this protection, ID Experts will help you resolve issues if your identity is compromised. We strongly encourage you to register for this free identity theft protection service. To enroll please visit: <https://www.idexpertscorp.com/enrollment/selectproductbefore.aspx?groupid=2707>

Your 12 month MyIDCare membership will include the following:

Complete Credit Monitoring and Recovery Services

- **Triple-Bureau Credit Monitoring** - Monitors any changes reported by Equifax, Experian, and TransUnion credit bureaus to your credit report.
- **Complete Recovery Services** - Should you believe that you are a victim of identity theft, ID Experts will work with you to assess, stop, and reverse identity theft issues.
- **Identity Theft Insurance** - In the event of a confirmed identity theft, you may be eligible for reimbursement of up to \$1,000,000 for expenses related to that theft.

Please note the deadline to enroll is Thursday, 30 November 2017.

I sincerely regret any inconvenience or concern that this matter may have caused you. Thank you for your patience and understanding while we work together to protect you. If you have any questions about this matter, please contact hr@greenriver.edu or Korland Simmons, Executive Assistant to the VP of HR & Legal Affairs at 253.288.3347.

-Marshall Sampson
VP of Human Resources & Legal Affairs
Green River College

Recommended Steps to help Protect your Information

Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

1. Website and Enrollment. Go to:

<https://www.idexperts.com/enrollment/selectproductbefore.aspx?groupid=2707>

and follow the instructions for enrollment. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive ID Experts' Member Website where you will find other valuable educational information.

2. Activate the credit monitoring provided as part of your membership with ID Experts. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, ID Experts will be able to assist you.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled with ID Experts, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with ID Experts, you will be contacted by a member of the Recovery Department who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Experts Recovery Advocate who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to \$5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.com/, Telephone: 1-919-716-6400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.