



September 4, 2015

Dear First Name Last Name,

I am writing to let you know of an incident that may affect the security of certain personal information relating to you and guidance on how you can protect yourself against the misuse of your personal information, should you feel it is necessary to do so.

What Happened? On August 24, 2015 we discovered a potential intrusion into our website server. We quickly moved to investigate this issue. In an abundance of caution, we took down the Agent of Change website on August 26, 2015. Third-party computer forensics experts were retained to assist with an investigation into the nature and scope of any intrusion. While the investigation is ongoing, it has been determined that there was unauthorized access to certain personal information relating to you, including your name, student ID number, email address (both the one provided by the school and any email provided by you upon registering), your Agent of Change username, your Agent of Change password, gender identity, race, ethnicity, age, relationship status, sexual identity and the name of your college or university.

What We Are Doing. In addition to taking down the Agent of Change website and working with third-party computer forensics, we have been working with our web developers to restore the site in a secure manner. We have also notified all of our affected clients about this incident and the steps we have taken since discovering this incident.

What You Can Do. While we do not have any evidence that the information related to you on the Agent of Change website has been misused, there are several steps you can take to protect yourself. We will require that you change the passwords associated with your Agent of Change account. We strongly encourage you to change your passwords for other accounts if your Agent of Change password is used elsewhere. Best practices for creating secure passwords include the following:

- Passwords should be complex and include the following:
 - Password must be 8-15 characters long
 - Password must contain at least 1 uppercase letter
 - Password must contain at least 1 lowercase letter
 - Password must include 1 special character (Examples: ! @ # \$ % ^ & * () _ -

+ = { []] | \ : ; \ " ' < , > . ? / ~ `)

- Passwords should be changed on a frequent schedule and individuals should have different passwords for each site that they visit.
- Review challenge question answers to see if they are on social media sites. Please be careful when selecting questions and answers as unauthorized users will mine data to try and guess answers to challenge questions.

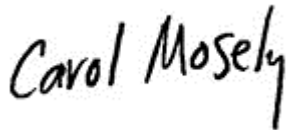
We also want to advise you to be on the look out for potential phishing emails. Phishing emails are typically attempting to steal personal information through legitimate-looking email messages from legitimate-looking email addresses. If you have received a suspected phishing email, please consider the following:

- Before clicking on a link, mouse over it to view the link address and ask yourself if it seems legitimate.
- Do not open or follow unsolicited/unexpected attachments or email links.
- If there is even a shred of doubt, forgo clicking on the link or attachment until you confirm that the link or attachment is legitimate.
- Do not provide a user ID or password in email, do not reply to emails asking you to send any personal information, and do not respond to emails that require you to enter personal or financial information directly into the email.

Additional steps you can take to protect yourself are included below.

The security of the personal information in our care is one of our highest priorities. We are sorry for the inconvenience this incident has caused you. If you have questions about the content of this email or about the incident, you can call 1-877-218-2930, 6 a.m. to 4 p.m. PST, Monday through Friday. Please provide reference number 6751090215 when calling.

Sincerely,



Carol Mosely

**ADDITIONAL STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT
AND FRAUD**

You may also take action directly to further protect against possible identity theft or other financial

loss. We encourage you to be vigilant by reviewing your account statements regularly and monitoring your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below. Information regarding security freezes is also available from these agencies.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

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

Consumers may place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place the freeze on all of your credit files.

To find out more on how to place a security freeze, you can visit the following sites:

Equifax Security Freeze - <http://freeze.equifax.com>

Experian Security Freeze - http://www.experian.com/consumer/security_freeze.html

TransUnion Security Freeze - <https://freeze.transunion.com>

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft/, 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. Instances of known or suspected identity theft should also be reported to law enforcement.

We End Violence LLC | 1286 University Ave #152 | San Diego, CA 92103-3312 US

If you not like to receive future notices from us, please [Opt-Out](#)