Actions you can take if you believe your Personally Identifiable Information (PII) may have been compromised:

- **Contact the credit bureaus.** Call or visit the websites of the three major credit bureaus (Equifax, Experian and TransUnion) and ask that they issue a fraud alert and attach a statement to your credit report. An initial alert can be placed on your account even if you merely think that you may become a victim. This alert will be placed in your file for 90 days, and states that you do not authorize an additional card on an existing account, an increase in the credit limit of an existing account, or new credit. You can get one free copy of your credit report from each bureau when you place an alert.
  
  - Equifax: 800-525-6285 or [www.equifax.com](http://www.equifax.com)
  - Experian: 888-397-3742 or [www.experian.com](http://www.experian.com)
  - TransUnion: 800-680-7289 or [www.transunion.com](http://www.transunion.com)

- **Review your credit reports.** After you receive your credit reports from the three credit bureaus, review them thoroughly. Make sure that all your personal information, including name, address, and Social Security number, is correct and that there are no fraudulent accounts or inquiries. Look for accounts that you didn’t apply for or open inquiries that you didn’t initiate, and defaults and delinquencies that you didn’t cause. Immediately report any suspicious information or activity to the credit bureau that issued the credit report.

- **Fill out an Identity Theft Victim’s Complaint and Affidavit.** The form is available from the Federal Trade Commission at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft). Creditors may accept this affidavit when you claim that you are not responsible for a new account or for transactions on an existing account. The information that you provide will enable the creditor to investigate your claim.

- **If the identification stolen is a government or school issued ID,** contact the agency or school that issued the document. Follow their procedures to cancel the document and get a replacement. Additionally, ask the agency or school to “flag” your file to keep anyone else from getting another identification document in your name.

- **Be Alert to Impersonators.** Make sure you know who is getting your personal or financial information. Don’t give out personal information on the phone, through the mail or over the Internet unless you’ve initiated the contact or know who you’re dealing with. If a company that claims to have an account with you sends email asking for personal information, don’t click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent the request. If you believe someone is using your lost or stolen information to impersonate you, report it to the company involved, as well as your local security officer.
• **Monitor your Social Networking Sites.** When identifying information has been lost or stolen, a thief can attempt to monitor social networking sites to gather additional information about you. If you post too much information about yourself, an identity thief can find information about your life, use it to answer ‘challenge’ questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.