What to do in the event of a data breach

Data Breaches are more and more common as identity thieves prove to be highly adept at obtaining confidential information from businesses and retail sites. If you are notified that a business you've patronized has experienced a data breach, first identify what information has been stolen, then consider taking the actions outlined below.

What information was lost or exposed?

Social Security Number

- If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- Review your credit report and check for errors. Check for any accounts or charges you don't recognize.
- Consider placing a credit freeze. A credit freeze makes it harder for someone to open a new account in your name.
    - If you decide not to place a credit freeze, consider placing a fraud alert.
- Try to file your taxes early--before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job.

Online login or password

- Log in to that account and change your password. If possible, also change your username.
    - If you can't login, contact the company. Ask them how you can recover or shut down the account.
- If you use the same password anywhere else, change that, too. Some scammers steal log-in information and try to use it on other websites.
- Is it a financial site, or is your credit card number stored? Check your account for any charges that you don't recognize.

Bank account, credit, or debit card information

- If your bank account was exposed, contact your bank to close the account and open a new one.
    - Consumers should also be aware of the Regulation E: Electronic Fund Transfer Act (EFTA), which provides guidelines for consumers and banks or other financial institutions in the context of electronic funds transfers.
    - These include transfers with automated teller machines (ATMs), point-of-sale transactions, and automated clearing house (ACH) systems.
    - Rules pertaining to consumer liability for unauthorized card usage fall under this regulation as well.
- If credit or debit card information was exposed, contact your credit card company to cancel your card and request a new one.
    - The Fair Credit Billing Act (FCBA) and the Electronic Fund Transfer Act (EFTA) offer protection if your credit, ATM, or debit cards are lost or stolen.
    - If someone makes unauthorized transactions with your debit card number, but your card is not lost, you are not liable for those transactions if you report them within 60 days of your statement being sent to you.

For more information on protecting yourself, please visit the **Identity Theft Center**. If you are a victim of identity theft call the toll free **Colorado Bureau of Investigation** 24 Hour Identity Theft & Fraud Hotline at 1-855-443-3489.

What to do in the event of a data breach

Major Credit Bureaus
TransUnion: www.transunion.com
P.O. Box 6790
Fullerton, CA 92834-6790 1-800-680-7289

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

Experian: www.experian.com
P.O. Box 9532
Allen, TX 75013
1-888-EXPERIAN (397-3742)

AFFECTED BY THE EQUIFAX BREACH? FILE A CLAIM NOW.
In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people. The company has agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement includes up to $425 million to help people affected by the data breach.

If your information was exposed in the data breach, you can file a claim at EquifaxBreachSettlement.com

Further information about the Equifax settlement can be found at http://ftc.gov/Equifax.

Beware! Scammers are already setting up fake websites that mimic the official websites for filing claims and getting information about the Equifax settlement. **If you are filing a claim, make absolutely sure that you are at the correct website** by looking at every letter of the web address and verifying it is correct. Verify that you have received the proper website address from a trusted source such as the Federal Trade Commission.