



Christopher E. Ballod, CIPP/US  
550 E. Swedesford Road, Suite 270  
Wayne, PA 19087  
[Christopher.Ballod@LewisBrisbois.com](mailto:Christopher.Ballod@LewisBrisbois.com)  
Direct: 215.977.4077

July 20, 2018

**VIA ELECTRONIC SUBMISSION**

Xavier Becerra, Attorney General  
Attorney General's Office  
California Department of Justice  
Attn: Public Inquiry Unit  
P.O. Box 944255  
Sacramento, CA 94244-2550

Re: Notification of Data Breach

Dear Attorney General Becerra:

I represent Institute on Aging, located in San Francisco, California. This letter is being sent pursuant to California Civil Code § 1798.82, because on May 28, 2018, Institute on Aging learned that an unauthorized individual may have accessed email accounts of Institute on Aging employees. We believe approximately 3,907 residents of California may have been affected. The incident may have involved unauthorized access to client and employees names, addresses, email addresses, dates of birth, financial records, and other health information including diagnosis, treatment, and medical payment information.

Institute on Aging immediately secured its systems and launched an investigation led by an expert team of data security response professionals. The Federal Bureau of Investigation was also notified in order to provide additional security and to prevent fraudulent activity. Institute on Aging also took additional measures to secure its systems and client and employee information to prevent similar incidents from occurring in the future.

Institute on Aging notified the affected California residents via the attached letter on July 20, 2018, and is providing twelve (12) months of complimentary credit and identity monitoring services to the affected residents through AllClear ID. Institute on Aging has also submitted the California Data Breach Reporting Form. Please contact me should you have any questions.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Chris Ballod'.

Christopher E. Ballod of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter; Data Security Breach Form


 00001  
ACD1234

 00001  
JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

July 20, 2018

**Subject: NOTICE OF DATA BREACH**

Dear John Sample,

<b>What Happened?</b>	<p>We are writing to you because of a recent security incident that occurred on May 28, 2018 at Institute on Aging (“IoA”). An unknown individual gained unauthorized access to some IoA employee email accounts, which may have contained personally identifiable information and/or protected health information.</p>
<b>What Information Was Involved?</b>	<p>The potentially compromised email accounts may have contained certain clients’ and employees’ names, addresses, phone numbers and email addresses, Social Security numbers, medical plan information, including health plan identification numbers and medical treatment information.</p>
<b>What We Are Doing:</b>	<p>We regret that this incident occurred and want to assure you that IoA is both adding additional security features to the affected systems in addition to other enhancements and is cooperating with federal authorities in investigating this incident. IoA is also reviewing and revising procedures and practices to minimize the risk of recurrence.</p>
<b>What You Can Do:</b>	<p>Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.</p> <p>Because your Social Security number may have been involved, to protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files and order copies of your credit reports by following the recommended privacy protection steps outlined in the enclosure. Check your credit reports for any accounts or medical bills that you do not recognize. If you find anything suspicious, follow the instructions found in step four of the enclosure.</p> <p>Since your health insurance information may have been involved, we recommend that you regularly review the explanation of benefits statement that you receive from your health insurance provider. If you see any service that you believe you did not receive, please contact your provider. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.</p> <p>As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.</p>



	<p>AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-682-4175 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.</p> <p>AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at <a href="http://enroll.allclearid.com">enroll.allclearid.com</a> or by phone by calling 1-855-682-4175 using the following redemption code: Redemption Code.</p> <p>Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.</p>
<b>Other Important Information:</b>	Enclosure "Breach Help –Consumer Tips from the California Attorney General"
<b>For More Information:</b>	For more information about privacy protection steps and your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at <a href="http://www.privacy.ca.gov">www.privacy.ca.gov</a> .
<b>Agency Contact:</b>	If you have questions please call AllClear ID at 1-855-682-4175, Monday through Saturday, 8:00 a.m. – 8:00 p.m. Central Time (excluding U.S. holidays).

*J. Thomas Briody, MHSc*

J. Thomas Briody, MHSc  
President and CEO

## STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

**Equifax**

P.O. Box 105851  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

**Experian**

P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**

P.O. Box 1000  
Chester, PA 19016  
1-877-322-8228  
[www.transunion.com](http://www.transunion.com)

**Free Annual Report**

P.O. Box 105281  
Atlanta, GA 30348  
1-877-322-8228  
[annualcreditreport.com](http://annualcreditreport.com)

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

**Security Freeze:** In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC at the address below or to the Attorney General in your state.

**Federal Trade Commission**

600 Pennsylvania Ave, NW  
Washington, DC 20580  
[consumer.ftc.gov](http://consumer.ftc.gov), and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

**Maryland Attorney General**

200 St. Paul Place  
Baltimore, MD 21202  
[oag.state.md.us](http://oag.state.md.us)  
1-888-743-0023

**North Carolina Attorney  
General**

9001 Mail Service Center  
Raleigh, NC 27699  
[ncdoj.gov](http://ncdoj.gov)  
1-877-566-7226

**Rhode Island**

**Attorney General**  
150 South Main Street  
Providence, RI 02903  
<http://www.riag.ri.gov>  
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.







# Breach Help

## Consumer Tips from the California Attorney General

Consumer Information Sheet 17 • October 2014

You get a letter from a company, a government agency, a university, a hospital or other organization. The letter says your personal information may have been involved in a data breach. Or maybe you learn about a breach from a news report or company web site. Either way, a breach notice does not mean that you are a victim of identity theft or other harm, but you could be at risk.

The breach notice should tell you what specific types of personal information were involved. It may also tell you what the organization is doing in response. There are steps you can take to protect yourself. What to do depends on the type of personal information involved in the breach.

Note that credit monitoring, which is often offered by breached companies, alerts you *after* someone has applied for or opened new credit in your name. Credit monitoring can be helpful in the case of a Social Security number breach. It does not alert you to fraudulent activity on your existing credit or debit card account.

### **Credit or Debit Card Number**

The breach notice should tell you when and where the breach occurred. If you used your credit or debit card at the location during the given time, you can take steps to protect yourself.

### **Credit Card**

1. Monitor your credit card account for suspicious transactions and report any to the card-issuing bank (or American Express or Discover). Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.
2. Consider cancelling your credit card if you see fraudulent transactions on it following the breach. You can dispute fraudulent

transactions on your credit card statement, and deduct them from the total due. Your liability for fraudulent transactions is limited to \$50 when you report them, and most banks have a zero-liability policy.<sup>1</sup>

3. If you do cancel your credit card, remember to contact any companies to which you make automatic payments on the card. Give them your new account number if you wish to transfer the payments.

### **Debit Card**

1. Monitor your debit card account for suspicious transactions and report any to the card issuer. Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.



2. Report any unauthorized transactions to your bank immediately to avoid liability. Your liability for fraudulent transactions is limited to \$50 if you report them within two days. Your bank may have a zero liability policy. But as time passes, your liability increases, up to the full amount of the transaction if you fail to report it within 60 days of its appearance on your bank statement.<sup>2</sup>
3. Consider cancelling your debit card. The card is connected to your bank account. Cancelling it is the safest way to protect yourself from the possibility of a stolen account number being used to withdraw money from your bank account. Even though it would likely be restored, you would not have access to the stolen money until after your bank has completed an investigation.

### **Social Security Number**

Here's what to do if the breach notice letter says your Social Security number was involved.

1. Contact the three credit bureaus. You can report the potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus. You will also be sent instructions on how to get a free copy of your report from each of the credit bureaus.

Experian	1-888-397-3742
Equifax	1-800-525-6285
TransUnion	1-800-680-7289

2. What it means to put a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that there may be fraud on the account. This

alerts the merchant to take steps to verify the identity of the applicant. A fraud alert lasts 90 days and can be renewed. For information on a stronger protection, a security freeze, see *How to Freeze Your Credit Files* at [www.oag.ca.gov/privacy/info-sheets](http://www.oag.ca.gov/privacy/info-sheets).

3. Review your credit reports. Look through each one carefully. Look for accounts you don't recognize, especially accounts opened recently. Look in the inquiries section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. You may find some inquiries identified as "promotional." These occur when a company has obtained your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (You are automatically removed from lists to receive unsolicited offers of this kind when you place a fraud alert.) Also, as a general precaution, look in the personal information section for any address listed for you where you've never lived.
4. If you find items you don't understand on your report, call the credit bureau at the number on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to contact the creditors involved and report the crime to your local police or sheriff's office.

### **Password and User ID**

In the case of an online account password breach, you may receive a notice by email or when you go to the log-on page for your account. Here are steps to take if you learn that your password and user ID or email address, or perhaps your security question and answer, were compromised.

1. Change your password for the affected account. If you find that you are locked out of your account, contact the company's customer service or security department.
2. If you use the same password for other accounts, change them too.
3. If a security question and answer was involved, change it. Don't use questions based on information that is publicly available, such as your mother's maiden name, your pet's name or the name of your high school.
4. Use different passwords for your online accounts. This is especially important for accounts that contain sensitive information, such as your medical or financial information. Consider accounts at online merchants where you may have your credit card number stored in the account.
5. Create strong passwords. Longer is better—at least ten characters long and a mix of uppercase and lowercase letters, numerals, punctuation marks, and symbols. Don't use words found in a dictionary. You can base passwords on a phrase, song or book title.  
*Example: "I love tropical sunsets" becomes 1luvtrop1calSuns3ts!*
6. A password manager or password "safe" can help you create and manage many strong passwords. These software programs can run on your computer, your phone and other portable devices. You only have to remember one password (or passphrase) to open the safe. The Electronic Frontier Foundation ([www.eff.org](http://www.eff.org)) lists some free versions and computer magazines offer product reviews.

### **Bank Information**

If the breach notice says your checking account number, on a check for example, was breached, here's what to do.

1. Call the bank, tell them about the breach and tell them you want to close your account. Find out what checks are outstanding. You may want to wait until they have cleared before closing the account. (Or you could write to each recipient, tell them about the breach, ask them not to process the old check and enclose a new check on your new account.)
2. Open a new bank account. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Ask your bank to notify the check verification company it uses that the old account was closed.

### **Driver's License Number**

If the breach notice says your driver's license or California identification card number was involved, and you suspect that you are a victim of identity theft, contact DMV's Driver License Fraud and Analysis Unit (DLFAU) by telephone at 1 866-658-5758 or by email at [dlfraud@dmv.ca.gov](mailto:dlfraud@dmv.ca.gov). Do not include personal information on your e-mail.

### **Medical or Health Insurance Information**

If the breach notice says your health insurance or health plan number was involved, here's what you can do to protect yourself against possible medical identity theft. A breach that involves other medical information, but not your insurance or plan number, does not generally pose a risk of medical identity theft.

1. If the letter says your Social Security number was involved, see section on Social Security number breaches. Also contact your insurer or health plan, as in number 2 below.
2. If the letter says your health insurance or health plan number was involved, contact





your insurer or plan. Tell them about the breach and ask them to note the breach in their records and to flag your account number.

3. Closely watch the Explanation of Benefits statements for any questionable items. An Explanation of Benefits statement comes in the mail, often marked "This is not a bill." It lists the medical services received by you or anyone covered by your plan. If you see a service that you did not receive, follow

up on it with your insurer or plan. For more on medical identity theft, see *First Aid for Medical Identity Theft: Tips for Consumers*, at [www.oag.ca.gov/privacy/info-sheets](http://www.oag.ca.gov/privacy/info-sheets).

For more details on what to do if you suspect that your information is being used to commit identity theft, see the *Identity Theft Victim Checklist* at [www.oag.ca.gov/idtheft/information-sheets](http://www.oag.ca.gov/idtheft/information-sheets).

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.

## NOTES

<sup>1</sup> Truth in Lending Act, 14 U.S. Code sec. 1601 and following.

<sup>2</sup> Electronic Funds Transfer Act, 15 U.S. Code sec. 1693 and following.

## AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

### **Services Provided**

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

### **Coverage Period**

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

### **Eligibility Requirements**

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

### **How to File a Claim**

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

### **Coverage under AllClear Identity Repair Does Not Apply to the Following:**

Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”);
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

### **Other Exclusions:**

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

### **Opt-out Policy**

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

<b>E-mail</b> support@allclearid.com	<b>Mail</b> AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	<b>Phone</b> 1.855.434.8077
---	--	--------------------------------







03931  
 TO THE ESTATE OF JOHN Q. SAMPLE  
 1234 MAIN STREET  
 ANYTOWN US 12345-6789

July 20, 2018

**Subject: NOTICE OF DATA BREACH**

To the Estate of John Sample,

<p><b>What Happened?</b></p>	<p>We are writing to you because of a recent security incident that occurred on May 28, 2018 at Institute on Aging (“IoA”). An unknown individual gained unauthorized access to some IoA employee email accounts, which may have contained personally identifiable information and/or protected health information.</p>
<p><b>What Information Was Involved?</b></p>	<p>The potentially compromised email accounts may have contained certain clients’ and employees’ names, addresses, phone numbers and email addresses, Social Security numbers, medical plan information, including health plan identification numbers and medical treatment information.</p>
<p><b>What We Are Doing:</b></p>	<p>We regret that this incident occurred and want to assure you that IoA is both adding additional security features to the affected systems in addition to other enhancements and is cooperating with federal authorities in investigating this incident. IoA is also reviewing and revising procedures and practices to minimize the risk of recurrence.</p>
<p><b>What You Can Do:</b></p>	<p>Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.</p> <p>Because your Social Security number may have been involved, to protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files and order copies of your credit reports by following the recommended privacy protection steps outlined in the enclosure. Check your credit reports for any accounts or medical bills that you do not recognize. If you find anything suspicious, follow the instructions found in step four of the enclosure.</p> <p>Since your health insurance information may have been involved, we recommend that you regularly review the explanation of benefits statement that you receive from your health insurance provider. If you see any service that you believe you did not receive, please contact your provider. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.</p> <p>As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.</p>



	<p>AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-682-4175 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.</p> <p>AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at <a href="http://enroll.allclearid.com">enroll.allclearid.com</a> or by phone by calling 1-855-682-4175 using the following redemption code: Redemption Code.</p> <p>Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.</p>
<b>Other Important Information:</b>	Enclosure "Breach Help –Consumer Tips from the California Attorney General"
<b>For More Information:</b>	For more information about privacy protection steps and your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at <a href="http://www.privacy.ca.gov">www.privacy.ca.gov</a> .
<b>Agency Contact:</b>	If you have questions please call AllClear ID at 1-855-682-4175, Monday through Saturday, 8:00 a.m. – 8:00 p.m. Central Time (excluding U.S. holidays).

*J. Thomas Briody, MHSc*

J. Thomas Briody, MHSc  
President and CEO

## STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

**Equifax**

P.O. Box 105851  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

**Experian**

P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**

P.O. Box 1000  
Chester, PA 19016  
1-877-322-8228  
[www.transunion.com](http://www.transunion.com)

**Free Annual Report**

P.O. Box 105281  
Atlanta, GA 30348  
1-877-322-8228  
[annualcreditreport.com](http://annualcreditreport.com)

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

**Security Freeze:** In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC at the address below or to the Attorney General in your state.

**Federal Trade Commission**

600 Pennsylvania Ave, NW  
Washington, DC 20580  
[consumer.ftc.gov](http://consumer.ftc.gov), and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

**Maryland Attorney General**

200 St. Paul Place  
Baltimore, MD 21202  
[oag.state.md.us](http://oag.state.md.us)  
1-888-743-0023

**North Carolina Attorney  
General**

9001 Mail Service Center  
Raleigh, NC 27699  
[ncdoj.gov](http://ncdoj.gov)  
1-877-566-7226

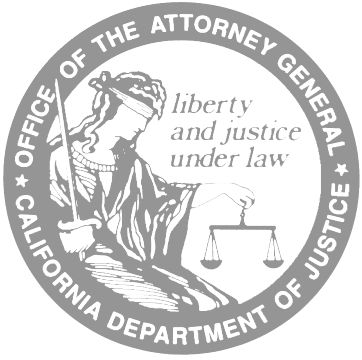
**Rhode Island**

**Attorney General**  
150 South Main Street  
Providence, RI 02903  
<http://www.riag.ri.gov>  
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.







# Breach Help

## Consumer Tips from the California Attorney General

Consumer Information Sheet 17 • October 2014

You get a letter from a company, a government agency, a university, a hospital or other organization. The letter says your personal information may have been involved in a data breach. Or maybe you learn about a breach from a news report or company web site. Either way, a breach notice does not mean that you are a victim of identity theft or other harm, but you could be at risk.

The breach notice should tell you what specific types of personal information were involved. It may also tell you what the organization is doing in response. There are steps you can take to protect yourself. What to do depends on the type of personal information involved in the breach.

Note that credit monitoring, which is often offered by breached companies, alerts you *after* someone has applied for or opened new credit in your name. Credit monitoring can be helpful in the case of a Social Security number breach. It does not alert you to fraudulent activity on your existing credit or debit card account.

### **Credit or Debit Card Number**

The breach notice should tell you when and where the breach occurred. If you used your credit or debit card at the location during the given time, you can take steps to protect yourself.

### **Credit Card**

1. Monitor your credit card account for suspicious transactions and report any to the card-issuing bank (or American Express or Discover). Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.
2. Consider cancelling your credit card if you see fraudulent transactions on it following the breach. You can dispute fraudulent

transactions on your credit card statement, and deduct them from the total due. Your liability for fraudulent transactions is limited to \$50 when you report them, and most banks have a zero-liability policy.<sup>1</sup>

3. If you do cancel your credit card, remember to contact any companies to which you make automatic payments on the card. Give them your new account number if you wish to transfer the payments.

### **Debit Card**

1. Monitor your debit card account for suspicious transactions and report any to the card issuer. Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.





2. Report any unauthorized transactions to your bank immediately to avoid liability. Your liability for fraudulent transactions is limited to \$50 if you report them within two days. Your bank may have a zero liability policy. But as time passes, your liability increases, up to the full amount of the transaction if you fail to report it within 60 days of its appearance on your bank statement.<sup>2</sup>
3. Consider cancelling your debit card. The card is connected to your bank account. Cancelling it is the safest way to protect yourself from the possibility of a stolen account number being used to withdraw money from your bank account. Even though it would likely be restored, you would not have access to the stolen money until after your bank has completed an investigation.

### **Social Security Number**

Here's what to do if the breach notice letter says your Social Security number was involved.

1. Contact the three credit bureaus. You can report the potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus. You will also be sent instructions on how to get a free copy of your report from each of the credit bureaus.

Experian	1-888-397-3742
Equifax	1-800-525-6285
TransUnion	1-800-680-7289

2. What it means to put a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that there may be fraud on the account. This

alerts the merchant to take steps to verify the identity of the applicant. A fraud alert lasts 90 days and can be renewed. For information on a stronger protection, a security freeze, see *How to Freeze Your Credit Files* at [www.oag.ca.gov/privacy/info-sheets](http://www.oag.ca.gov/privacy/info-sheets).

3. Review your credit reports. Look through each one carefully. Look for accounts you don't recognize, especially accounts opened recently. Look in the inquiries section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. You may find some inquiries identified as "promotional." These occur when a company has obtained your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (You are automatically removed from lists to receive unsolicited offers of this kind when you place a fraud alert.) Also, as a general precaution, look in the personal information section for any address listed for you where you've never lived.
4. If you find items you don't understand on your report, call the credit bureau at the number on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to contact the creditors involved and report the crime to your local police or sheriff's office.

### **Password and User ID**

In the case of an online account password breach, you may receive a notice by email or when you go to the log-on page for your account. Here are steps to take if you learn that your password and user ID or email address, or perhaps your security question and answer, were compromised.

1. Change your password for the affected account. If you find that you are locked out of your account, contact the company's customer service or security department.
2. If you use the same password for other accounts, change them too.
3. If a security question and answer was involved, change it. Don't use questions based on information that is publicly available, such as your mother's maiden name, your pet's name or the name of your high school.
4. Use different passwords for your online accounts. This is especially important for accounts that contain sensitive information, such as your medical or financial information. Consider accounts at online merchants where you may have your credit card number stored in the account.
5. Create strong passwords. Longer is better—at least ten characters long and a mix of uppercase and lowercase letters, numerals, punctuation marks, and symbols. Don't use words found in a dictionary. You can base passwords on a phrase, song or book title.  
*Example: "I love tropical sunsets" becomes 1luvtrop1calSuns3ts!*
6. A password manager or password "safe" can help you create and manage many strong passwords. These software programs can run on your computer, your phone and other portable devices. You only have to remember one password (or passphrase) to open the safe. The Electronic Frontier Foundation ([www.eff.org](http://www.eff.org)) lists some free versions and computer magazines offer product reviews.

### **Bank Information**

If the breach notice says your checking account number, on a check for example, was breached, here's what to do.

1. Call the bank, tell them about the breach and tell them you want to close your account. Find out what checks are outstanding. You may want to wait until they have cleared before closing the account. (Or you could write to each recipient, tell them about the breach, ask them not to process the old check and enclose a new check on your new account.)
2. Open a new bank account. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Ask your bank to notify the check verification company it uses that the old account was closed.

### **Driver's License Number**

If the breach notice says your driver's license or California identification card number was involved, and you suspect that you are a victim of identity theft, contact DMV's Driver License Fraud and Analysis Unit (DLFAU) by telephone at 1 866-658-5758 or by email at [dlfraud@dmv.ca.gov](mailto:dlfraud@dmv.ca.gov). Do not include personal information on your e-mail.

### **Medical or Health Insurance Information**

If the breach notice says your health insurance or health plan number was involved, here's what you can do to protect yourself against possible medical identity theft. A breach that involves other medical information, but not your insurance or plan number, does not generally pose a risk of medical identity theft.

1. If the letter says your Social Security number was involved, see section on Social Security number breaches. Also contact your insurer or health plan, as in number 2 below.
2. If the letter says your health insurance or health plan number was involved, contact



your insurer or plan. Tell them about the breach and ask them to note the breach in their records and to flag your account number.

3. Closely watch the Explanation of Benefits statements for any questionable items. An Explanation of Benefits statement comes in the mail, often marked "This is not a bill." It lists the medical services received by you or anyone covered by your plan. If you see a service that you did not receive, follow

up on it with your insurer or plan. For more on medical identity theft, see *First Aid for Medical Identity Theft: Tips for Consumers*, at [www.oag.ca.gov/privacy/info-sheets](http://www.oag.ca.gov/privacy/info-sheets).

For more details on what to do if you suspect that your information is being used to commit identity theft, see the *Identity Theft Victim Checklist* at [www.oag.ca.gov/idtheft/information-sheets](http://www.oag.ca.gov/idtheft/information-sheets).

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.

## NOTES

<sup>1</sup> Truth in Lending Act, 14 U.S. Code sec. 1601 and following.

<sup>2</sup> Electronic Funds Transfer Act, 15 U.S. Code sec. 1693 and following.

## AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

### **Services Provided**

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

### **Coverage Period**

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

### **Eligibility Requirements**

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

### **How to File a Claim**

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

### **Coverage under AllClear Identity Repair Does Not Apply to the Following:**

Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”);
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

### **Other Exclusions:**

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

### **Opt-out Policy**

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

<b>E-mail</b> support@allclearid.com	<b>Mail</b> AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	<b>Phone</b> 1.855.434.8077
---	--	--------------------------------



