Lawrence S. Gordon (CA Bar No. 302330)
COZEN O'CONNOR
101 Montgomery Street, Suite 1400
San Francisco, CA 94104
Tel: 415.644.0914
Fax: 415.644.0978
Email: lgordon@cozen.com

Anthony Pinggera (CA Bar No. Pending)
LAMBDA LEGAL DEFENSE & EDUCATION FUND, INC.
4221 Wilshire Boulevard, Suite 280
Los Angeles, CA 90010
Tel: 213.382.7600
Email: apinggera@lambdalegal.org

Scott Schoettes (IL Bar No. 6282105)
Jamie A. Gliksberg (IL Bar No. 6309091)
(*Pro Hac Vice* Motions Pending)
LAMDA LEGAL DEFENSE & EDUCATION FUND, INC.
105 West Adams, 26th Floor
Chicago, IL 60603-6208
Tel: 312.663.4413
Email: sschoettes@lambdalegal.org
Email: jgliksberg@lambdalegal.org

Attorneys for Plaintiff, A. DOE

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN FRANCISCO

A. DOE, individually and on behalf of all others similarly situated,

Plaintiff(s),

v.

A.J. BOGGS & COMPANY,

Defendant.

Case No.: _____

CLASS ACTION COMPLAINT FOR DAMAGES

1. Violation of the California AIDS Public Health Records Confidentiality Act (Health & Safety Code § 121025)

2. Violation of Confidentiality of Medical Information Act (Civil Code § 56, *et seq.*)

[Jury Trial Demanded]

CLASS ACTION COMPLAINT

Plaintiff ALAN DOE ("Plaintiff"), a pseudonym used to protect the privacy of the named plaintiff, brings this class action on behalf of himself and all others similarly situated against defendant A.J. Boggs & Company ("A.J. Boggs") and alleges as follows:

INTRODUCTION

1. This class action is brought to vindicate the privacy rights of Plaintiff and all other persons living with HIV whose identities, personal data, and medical information were accessed by unauthorized individuals because Defendant A.J. Boggs failed to adequately protect and secure this highly sensitive information.

2. Between August 2016 and November 2016, Plaintiff and the putative class members were participants in California's AIDS Drug Assistance Program ("ADAP"). The program participants relied on A.J. Boggs, the company contracted to administer program enrollment, to aid them in procuring life-saving medications to keep HIV under control.

3. Plaintiff and other program participants trusted A.J. Boggs—and A.J. Boggs had a legal obligation—to keep their personal medical information, including their identities as HIV-positive individuals, strictly confidential.

4. Instead of treating the private health information of its clients with the care it was due, A.J. Boggs left the database containing this information open to exploitation. As a result of A.J. Boggs's negligent or willful conduct, ninety-three participants in California's ADAP program had their private information accessed by individuals who subsequently could reveal participants' HIV status to an unknown number of additional individuals.

5. Public health officials and others working in the field understand that HIV-related stigmas are key drivers of the HIV/AIDS epidemic. Such stigmas disincentivize people from

learning their HIV status, discourage them from engaging in care after being diagnosed with HIV, and make it more difficult for those engaged in care to remain adherent to their HIV medications.

6. While HIV-related stigma has abated somewhat within the general population, it has been dishearteningly persistent—particularly within communities most affected by the disease—even as scientific and medical knowledge about HIV and our collective ability to combat the disease have grown exponentially.

7. The California AIDS Public Health Records Confidentiality Act and the California Confidentiality of Medical Information Act provide important protections for people living with HIV as a bulwark against the public disclosure of confidential medical information that is potentially highly stigmatizing.

8. Though more people are making the choice to live openly with HIV today than ever before, this statutory scheme ensures that people living with HIV—as well as those living with other stigmatized medical conditions—are in control of their personal and private medical information and are allowed to choose to whom and when they disclose this extremely sensitive information.

9. A.J. Boggs's ineptitude took that choice away from Plaintiff and other program participants, compromised the confidentiality of their medical information, and violated the trust placed in A.J. Boggs to protect program participants' privacy regarding their HIV status.

JURISDICTION AND VENUE

10. This Court has jurisdiction over Defendant A.J. Boggs because it is a corporation authorized to do business in California that conducts substantial business in the State, and all claims arise from A.J. Boggs's activity within the State.

11. Venue is proper in San Francisco County under California Code of Civil Procedure § 395 because Defendant does not reside in the State, enabling this action to be tried in the superior court in any county that Plaintiff designates in the complaint.

PARTIES

12. Plaintiff is a resident and domiciliary of the State of California, and is a person living with HIV. At all times relevant to this action, Plaintiff was enrolled in California's AIDS Drug Assistance Program, a federally funded program to help manage the cost of his HIV treatment.

13. Defendant A.J. Boggs & Company was the private contractor responsible for administering California's ADAP enrollment services from April 2016 to March 2017. A.J. Boggs has its headquarters in East Lansing, MI.

STATEMENT OF FACTS

14. Under the Ryan White CARE Act, 42 U.S.C. § 300ff *et seq*., each state is eligible to receive federal funding to conduct a program that helps ensure access to HIV medications for lower-income people living with HIV who are not eligible for Medicaid and do not have an alternative source to obtain HIV medications at a reasonable cost. A program authorized under this section of the Ryan White CARE Act is called an AIDS Drug Assistance Program. 42 U.S.C. § 300ff-21 *et seq*.

15. California has approximately 30,000 people, including Plaintiff, enrolled in its ADAP. At all relevant times, all people enrolled in California's ADAP were people living with HIV.

16. Enrollment in ADAP requires applicants to provide detailed information about their HIV-related health care, as well as access to their medical records.

17. Prior to March 2017, the State of California contracted with a private vendor selected through a bidding process to administer the State's ADAP.

18. Based on information and belief, from 1997 to 2016, California's ADAP was administered solely by Ramsell Corporation ("Ramsell").

19. Prior to the expiration of Ramsell's contract with the State in 2016, the California Department of Public Health ("CDPH") decided to restructure its ADAP administration system by dividing various functions among different entities.

20. In the ensuing bidding process, A.J. Boggs was chosen to administer the enrollment services for California's ADAP. As the ADAP enrollment contractor, A.J. Boggs was privy to Plaintiff's private health information.

21. As a custodian of the private health information of its clients, the ADAP administrator is required by state law to ensure that such information is not disclosed or disseminated without the clients' consent.

22. Among the services that A.J. Boggs was contracted to provide was an "ADAP enrollment portal." The ADAP enrollment portal allows case managers to enroll clients in ADAP, to enter aspects of their clients' private medical information into the system, and to subsequently access the private health information of individuals enrolled through the organization for which the case manager works. A.J. Boggs chose to build this online ADAP enrollment and management system itself from the ground up.

23. Upon information and belief, A.J. Boggs expected to make its enrollment services platform, including the ADAP enrollment portal, fully functional on July 1, 2016.

24. On April 6, 2016, several nonprofits whose staff members enroll community members in ADAP wrote a letter to CDPH articulating their concerns about the proposed rollout of a new ADAP enrollment system. One important concern was that the enrollment system, less than twelve weeks from launching, had not been beta tested to ensure its functionality and security.

25. On June 14, 2016, those same nonprofits wrote a second letter to CDPH, this time explicitly requesting a three-month delay of the rollout of A.J. Boggs's ADAP enrollment system.

With less than three weeks before the system went live, the nonprofits reiterated their concern that the new system was still not beta tested.

26. The next day, on June 15, 2016, the Los Angeles County Department of Public Health sent a letter to CDPH voicing the same concerns about the lack of testing and requesting a six-month delay in the rollout of the new system.

27. CDPH provided assurances to the HIV nonprofits that the new enrollment system would be fully functional by the rollout date. In spite of the repeated protestations of community stakeholders, A.J. Boggs introduced the new enrollment system as scheduled on July 1, 2016.

28. The new ADAP enrollment system began experiencing problems almost immediately, including treatment interruptions for clients, inadequate communication between A.J. Boggs and the pharmacy benefits contractor, and overall poor system functionality.

29. On information and belief, a security vulnerability in the enrollment portal was exploited on August 16, 2016, and the private health information of ADAP clients, including Plaintiff, was left vulnerable to unauthorized third-party access. On information and belief, this security vulnerability went unnoticed by A.J. Boggs until November 2016.

30. On November 29, 2016, the online enrollment portal was taken offline due to the information security vulnerabilities in the system.

31. On December 7, 2016, the security vulnerability allegedly was fixed. However, based on information and belief, the online enrollment portal created by A.J. Boggs was never brought back online for use by case managers or other enrollment workers.

32. On information and belief, on or about February 7, 2017, CDPH discovered that sometime between August 16, 2017, and December 7, 2017, unauthorized third parties accessed Plaintiff's private health information, along with the private health information of at least ninety-two other ADAP clients.

33. The private health information of at least ninety-three specific ADAP clients, including Plaintiff, was improperly accessed and viewed by at least one unauthorized third party between July 2016 and November 2016.

34. On information and belief, CDPH hired a consulting firm to investigate, analyze and report on the breaches that occurred.

35. According to CDPH, the investigation identified the IP addresses of the third parties who accessed the private medical information, but the consulting firm was unable to uncover their locations or identities.

36. On March 1, 2017, CDPH announced it was cancelling its contract with A.J. Boggs, effective March 31, 2017. On March 6, 2017, CDPH began processing ADAP enrollment applications on its own, without the assistance of an outside contractor.

37. Plaintiff received a letter on April 7, 2017, alerting him that his private health information, along with the private health information of ninety-two other people, was improperly accessed by at least one unauthorized third party. *See* Exhibit 1.

38. Identification of Plaintiff in the ADAP enrollment database would necessarily reveal his HIV status to any outside party accessing that database.

39. A person's HIV status is singularly sensitive information and sharing that status with others is an intensely personal choice. Any person living with HIV should have full control over when and with whom this information is shared. However, as a result of A.J. Bogg's failures, knowledge of Plaintiff's HIV status is now in the hands of unauthorized, unknown persons. In addition to breaching the trust of ADAP participants and their caseworkers, A.J. Boggs's conduct violated two California statutes.

CLASS ACTION ALLEGATIONS

40. Plaintiff brings this action pursuant to California Code of Civil Procedure § 382 and Civil Code § 1781, on behalf of himself and all others similarly situated (the "Class"), and seeks certification of a Class consisting of: all persons residing in the State of California whose personal information was held in the ADAP portal and accessed by unauthorized persons between July 2016 and November 2016. Excluded from the Class is Defendant, including any of its officers, directors, employees, affiliates, legal representatives, attorneys, heirs, and assigns, and any entity in which Defendant has a controlling interest. Judicial officers presiding over this case, its staff, and immediate family members, are also excluded from the Class.

41. *Numerosity.* The members of the Class are so numerous that their individual joinder is impractical. While the exact number of Class members is unknown to Plaintiff at this time, Plaintiff is informed and believes, and on that basis alleges, that the proposed Class contains at least ninety-three members. Joinder is made more impractical by the fact that the identities of these individuals are unknown, that their status as people living with HIV make their identities subject to additional confidentiality restrictions, and that many of them—for obvious reasons—may not want to step forward in public to advance their rights to privacy and confidentiality through a lawsuit. Defendant is able to ascertain the precise size of the Class and possesses records that include the contact information for all Class members, enabling proper notice to all Class members of the pendency of this action.

42. *Predominance and Commonality.* Defendant violated the State of California's medical privacy laws relative to the entire Class, giving rise to common questions of law and fact of common or general interest to all Class members' claims for relief. Common questions of law and fact predominate over any potential questions affecting only individual Class members, including, but not limited to, the following:

a. Whether Defendant was negligent in storing, maintaining, preserving, securing, and encrypting Plaintiff's and Class members' private information in violation of Civil Code § 56.101;

b. Whether Defendant negligently or willfully disclosed or released Plaintiff's and Class members' private information to unauthorized persons in violation of Health and Safety Code § 121025;

c. Whether Plaintiff and Class members are entitled to statutory damages and/or civil penalties;

d. Whether Plaintiff and Class members are entitled to recover their costs and attorneys' fees related to this class action.

43. *Typicality.* Plaintiff's claims are typical of those of all other Class members because Defendant disclosed, misused, or improperly allowed access to Plaintiff's and the entire Class's private information. Plaintiff suffers from the same violations of the State of California's medical privacy laws as all other Class members, their claims for relief are based on the same legal theories and result from Defendant's same unlawful conduct, and their injuries are the same.

44. *Adequacy of Representation.* Plaintiff's claims are typical of all Class members' claims and Plaintiff can and will fairly and adequately represent and protect the interests of all Class members. Plaintiff retained competent counsel with substantial experience in litigating complex consumer class actions as well as HIV-related privacy breaches, and Plaintiff, represented by counsel, is committed to prosecute this action vigorously. Neither Plaintiff nor its counsel have any adverse interests to the rest of the Class.

45. *Superiority.* A class action is superior to all other available means of fairly and efficiently adjudicating this controversy since individual litigation of the claims for each Class member would be impracticable. The burdens and expenses of individual litigation for each Class

member would be prohibitively high relative to the small potential for recovery available to each Class member. Denial of class certification, therefore, would cause Class members' injuries, which include substantial damages in the aggregate, to go unremedied. It would also be unduly burdensome on the Court to litigate all Class members' claims individually in spite of their same factual issues. The as-yet-unknown identities of other Class members, along with the additional confidentiality concerns inherent in the case, makes joinder impractical. There are no known or anticipated difficulties in managing this litigation as a class action that would preclude it from proceeding in this manner. Individual litigation of Class members' claims would result in repetitive adjudication of common questions of law and fact that could create inconsistent, varying, or contradictory judgments and establish incompatible or inconsistent standards of conduct.

46. This action is suitable to be litigated as a class action under Code of Civil Procedure § 382 since the Class is easily ascertainable and there exists a well-defined community of interest in the litigation.

FIRST COUNT

Violations of the California AIDS Public Health Records Confidentiality Act (California Health & Safety Code § 121025)

47. Plaintiff reincorporates the previous allegations as if fully set forth herein.

48. Defendant was an agent of the California Department of Public Health. As an agent of a state public health agency, Defendant is subject to the requirements of the California AIDS Public Health Records and Confidentiality Act, Cal. Health & Safety Code § 121025.

49. Plaintiff and Class members entrusted Defendant with individualized private health information, including their HIV status. Defendant had a legal duty to preserve the confidentiality of the records of Plaintiff and Class members.

50. The private health information that Plaintiff and Class members entrusted to Defendant, including their status as individuals living with HIV, that Defendant negligently,

willfully, or maliciously disclosed constituted "confidential public health records" within the meaning of Health & Safety Code § 121035. Defendant had an obligation to prevent the disclosure of this information to unauthorized third parties without written authorization from Plaintiff or Class members.

51. Defendant's improper conduct with respect to this private information made it accessible, available, viewable and/or downloadable over the internet to unauthorized individuals. The private health information of Plaintiff and ninety-two others was in fact improperly accessed by at least one or more unauthorized individuals as a result of Defendant's wrongful conduct.

52. As a direct and proximate result of Defendant's acts and omissions in violation of § 121025, Plaintiff and Class members were injured within the meaning of the California AIDS Public Health Records Confidentiality Act and are entitled to civil penalties of up to $25,000 each plus court costs pursuant to § 121025(e)(1).

SECOND COUNT

Violations of the California Confidentiality of Medical Information Act (California Civil Code § 56 *et seq*.)

53. Plaintiff reincorporates the previous allegations as if fully set forth herein.

54. Defendants are subject to the requirements and mandates of the California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56 *et seq.* ("CMIA").

55. As a healthcare contractor, Defendant is subject to the confidentiality requirements of § 56.101 of the CMIA.

56. Under § 56.101 of the CMIA, health care providers and contractors are required to maintain, preserve, and store medical information "in a manner that preserves the confidentiality of the information contained therein." Electronic medical record systems are required to "protect and preserve the integrity of electronic medical information."

57. The negligent maintenance or storage of medical information by a contractor is prohibited, and contractors who negligently maintain their systems are liable for damages and penalties under Civil Code § 56.36.

58. Under § 56.36 of the CMIA, a person or entity that knowingly and willfully obtains and discloses medical information of in violation of that section is liable for a civil penalty not to exceed $25,000 per violation.

59. Plaintiff and Class members entrusted Defendant with their private information and, at all relevant times, Defendant had a legal duty to protect and exercise reasonable care in preserving the confidentiality of Plaintiff's and other Class members' private information.

60. The private information, which included Plaintiff and Class members' HIV status, was improperly accessed and viewed by one or more unauthorized individuals as a result of Defendant's wrongful conduct as set forth above.

61. Plaintiff's and Class members' private information was accessed and viewed without ever obtaining their authorization for the disclosure of such information.

62. Defendant negligently created, maintained, preserved, and stored Plaintiff's and Class members' private medical information, and/or obtained and knowingly and willfully disclosed Plaintiff's and Class members' private medical information without their written authorization.

63. As a direct and proximate result of Defendant's acts and omissions in violation of § 56.101, Plaintiff and Class members were injured within the meaning of the CMIA and are entitled to statutory damages of $1,000 each, as well as any actual damages suffered by Plaintiff and the Class members as a result of Defendant's conduct, pursuant to § 56.36(b).

64. Pursuant to § 56.36(c), Defendant is also liable, irrespective of the damage to Plaintiff and the Class members, in the form of a civil penalty of up to $25,000 per violation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays that this Court grant the following relief:

A. Certify this action as a class action and appoint Plaintiff and his counsel to represent the Class;

B. Award statutory damages and actual damages;

C. Impose civil penalties and court costs as specified in the respective statutes;

D. Award Plaintiff and Class members their reasonable costs and attorneys' fees;

E. Grant any other and further relief that this Court may deem fit and proper.

Respectfully submitted,

By: _____

Lawrence S. Gordon (CA Bar No. 302330)
COZEN O'CONNOR
101 Montgomery Street, Suite 1400
San Francisco, CA 94104
Tel: 415.644.0914
Fax: 415.644.0978
Email: lgordon@cozen.com

Anthony Pinggera (CA Bar No. Pending)
LAMBDA LEGAL DEFENSE & EDUCATION FUND, INC.
4221 Wilshire Boulevard, Suite 280
Los Angeles, CA 90010
Tel: 213.382.7600
Email: apinggera@lambdalegal.org

Scott Schoettes (IL Bar No. 6282105)
Jamie A. Gliksberg (IL Bar No. 6309091)
(*Pro Hac Vice* Motions Pending)
LAMDA LEGAL DEFENSE & EDUCATION FUND, INC.
105 West Adams, 26th Floor
Chicago, IL 60603-6208
Tel: 312.663.4413
Email: sschoettes@lambdalegal.org
Email: jgliksberg@lambdalegal.org

Attorneys for Plaintiff, A. DOE

Dated: April 3, 2018

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all claims to the extent authorized by law.

Respectfully submitted,

By: _____

Lawrence S. Gordon (CA Bar No. 302330)
COZEN O'CONNOR
101 Montgomery Street, Suite 1400
San Francisco, CA 94104
Tel: 415.644.0914
Fax: 415.644.0978
Email: lgordon@cozen.com

Anthony Pinggera (CA Bar No. Pending)
LAMBDA LEGAL DEFENSE & EDUCATION FUND, INC.
4221 Wilshire Boulevard, Suite 280
Los Angeles, CA 90010
Tel: 213.382.7600
Email: apinggera@lambdalegal.org

Scott Schoettes (IL Bar No. 6282105)
Jamie A. Gliksberg (IL Bar No. 6309091)
(*Pro Hac Vice* Motions Pending)
LAMDA LEGAL DEFENSE & EDUCATION FUND, INC.
105 West Adams, 26th Floor
Chicago, IL 60603-6208
Tel: 312.663.4413
Email: sschoettes@lambdalegal.org
Email: jgliksberg@lambdalegal.org

Attorneys for Plaintiff, A. DOE

Dated: April 3, 2018

Exhibit 1

State of California—Health and Human Services Agency
California Department of Public Health

KAREN L. SMITH, MD, MPH
Director and State Public Health Officer

EDMUND G. BROWN JR.
Governor

4/7/2017

REDACTED

Dear REDACTED: **Notice of Data Breach**

This letter is to notify you that on or about February 7, 2017, the California Department of Public Health (Department) determined that some personal information, including personal health information, about you may have been improperly accessed via an Enrollment website built and maintained by a Department contractor. While our investigation is still ongoing, we wanted to make you aware of this potential breach. The Department will provide you additional details when the investigation is finalized. The Department has terminated its contract with the contractor involved. We recognize this is a frustrating process and deeply regret that this data breach occurred. We apologize for any inconvenience it has caused you and other Department clients.

What happened?
In 2016, the Department became aware that the Enrollment website, administered by the Department's contractor, may have lacked adequate controls and safeguards required to protect the privacy and security of personal information of program clients. Because of the risk to personal information posed by these security vulnerabilities in the Enrollment website, the Department shut down access to the Enrollment website after learning of the vulnerabilities and began an investigation of security issues in connection with the Enrollment website.

The Department has determined that its contractor did not have in place adequate personal information security controls and failed to take other measures to protect the personal information of Department program clients, as required by its contract with the Department.

Our ongoing investigation indicates that personal information, including personal health information, about you may have been accessed by an unauthorized individual(s) between August 16, 2016 and December 7, 2016.

The Department's investigation has been unable to determine whether your personal information may have been accessed by one individual or more than one individual, and is unable to identify the identity of the individual(s) who may have improperly accessed your information.

What information was involved?
The information about you that may have been inappropriately accessed may include your health status, name, Social Security number, date of birth, and enrollment site number.

What we are doing?
We regret that this incident occurred, and we have taken steps to ensure that no inappropriate access to your personal information occurs, including termination of our contract with the contractor involved.

What you can do
In order to help protect you from the possibility of identity theft, we are offering you fraud detection and credit monitoring services at no cost to you. These credit monitoring services are available to you through February 26, 2018. Please call the Department Contact (see below) for information on how to activate and use your free fraud detection and credit monitoring services.

Other important information
Enclosure "Breach Help –Consumer Tips from the California Attorney General"

For more information
For information about your privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection Unit at www.privacy.ca.gov.

Department contact
Should you need any further information about this incident, please contact the Department's call center at (844) 421-7050.

Sincerely,

Karen L. Smith, MD, MPH
Director and State Public Health Officer

Enclosure: "Breach Help – Consumer Tips from the California Attorney General"

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.[1]

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.

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*) 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*. 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