

North Carolina Security Breach Reporting Form Pursuant to the Identity Theft Protection Act of 2005

Name of Business Owning or Licensing Information Affected by the Breach: Pillsbury Winthrop Shaw Pittman
 Address: 50 Fremont Street
San Francisco, CA 94120-7880
 Telephone: 415-983-1000
 Fax: 415-983-1200
 Email: deborah.johnson@pillsburylaw.com

PLEASE SUBMIT FORM TO:
 Consumer Protection Division
 NC Attorney General's Office
 9001 Mail Service Center
 Raleigh, NC 27699-9001
 Telephone: (919) 716-6000
 Toll Free in NC: (877) 566-7226
 FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: July 25, 2008
 Date the Security Breach was discovered: Notice of breach received from vendor 6/15/08
 Estimated number of affected individuals: 3392
 Estimated number of NC residents affected: 10

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): Colt Express Outsourcing Services, Inc.
2125 Oak Grove Road, Walnut Creek, CA 94598-3400

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: Electronic data (name, address, birthdate, SSN) was on computers/servers stolen from Colt's offices. Data was password protected, not encrypted. Theft discovered 5-27-08.

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. unknown If so, please describe the security measures protecting the information: _____

Describe any measures taken to prevent a similar Security Breach from occurring in the future: Colt advised it installed an alarm system. Pillsbury terminated Colt services in 2002.

Date affected NC residents were/will be notified: Notifications being mailed July 29, 2008

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): On receipt of notice from Colt on 6/16/08, Pillsbury has been working to verify affected individuals and confirm contact information.

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))
 Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

written notice
 electronic notice (email)
 telephone notice
 substitute notice

Signature: Deborah Johnson Date: July 25, 2008
 Contact Person, Title: Deborah Johnson, Chief Human Resources Officer
 Address: _____
 (if different from above) _____
 Telephone: _____ Fax: _____ Email: _____



Secure Processing Center | 600 Satellite Blvd | Suwanee, GA 30024

Urgent Message from Pillsbury. Please Open Immediately.

<FirstNames> <MiddleInitials> <LastNames> <Suffix>

<Date (Month Day, Year)>

<Address> (Line 1)

<Address> (Line 2)

<City> <State> <Zip>

<POSTNET BARCODE>

Re: Notice of Potential Data Security Breach

Dear <FirstNames> <MiddleInitials> <LastNames> <Suffix>:

I am writing to let you know of a recent event that may affect you. Regrettably, we have been informed that on May 26, 2008, a break-in and theft of computers, containing personal information, occurred at the offices of one of our former external benefit administration vendors, Colt Express Outsourcing Services, Inc. ("Colt") in Walnut Creek, CA. Colt handled benefits plan billing in 1998, and COBRA administration from mid-1998 to mid-2002. This personal information included your name, address, birth date, and Social Security number. If we provided benefits to your dependents, their personal information may also have been exposed by this incident. We were notified of this situation by letter on about June 16 and have been working diligently to determine what information and which individuals may have been affected.

Even though we do not know whether your personal information has been improperly accessed or misused, we want to make you aware of the incident and the steps that have been taken to prevent a reoccurrence. First, upon discovery the next morning, Colt reported the theft to the Walnut Creek, California Police Department. Colt also commenced an investigation to determine the extent to which customer data was likely stored on the stolen equipment. We have taken additional measures to protect information regarding you that we maintain, and we are also working with our past and current vendors to fortify security practices already in place to prevent future potential security breaches.

In addition, to safeguard against any possible misuse of your personal information, we have engaged Kroll Inc. to provide you with access to its ID TheftSmart™ service through July 2009. This service includes Continuous Credit Monitoring and a Trimerged Credit Report at no cost to you. Should you suspect that you may be a victim of identity fraud, you will have access to Kroll's Licensed Investigators for guidance and consultation.

Information about ID TheftSmart's comprehensive program is enclosed; we encourage you to take the time to read about the safeguards now available to you. If you choose to take advantage of Kroll's ID TheftSmart credit services, please complete and return the enclosed authorization form as soon as possible. If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services at 1-800-XXX-XXXX between 8:00 a.m. and 5:00 p.m. (Central Time), Monday through Friday.

You have the right to obtain a copy of your credit report for free once a year from each credit reporting agency whether or not you suspect any unauthorized activity. You can obtain a free credit report by contacting one of the agencies listed below or by visiting www.annualcreditreport.com or by calling 1-877-322-8228. The law allows you to order a free credit report from each agency every 12 months. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to keep an eye on the accuracy and completeness of the information in your reports. Just call one of the numbers below to order your report.

You also have the right to place an initial "fraud alert" on your credit file. A "fraud alert" lets creditors know that they should contact you before they open a new account in your name. You can do this by calling any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts with all three agencies, who will send you information on how you can order a free credit report from each of the agencies. The "fraud alert" will stay on your account for 90 days. After that you can renew the alert for additional 90 day periods by calling any one of the three agencies:

- Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241;
- Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 2002, Allen, TX 75013; and
- TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

When you receive your credit report, look it over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. Look for personal information, such as home address, employment or social security numbers, which is not accurate. If you see anything you do not understand call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit report, call your local police or sheriff's office and the Federal Trade Commission and file a report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit reports every three or four months for the next year. For more information on identity theft, we suggest that you contact the California Office of Privacy Protection, whose toll-free number is 866-785-9663. You can visit their website at www.privacy.ca.gov. You can contact the Federal Trade Commission at 1-877-FTC-HELP (1-877-382-4357). The FTC website has a special section on identity theft offers helpful information. That site is www.consumer.gov/idtheft/.

Maryland residents can obtain more information about identity theft by contacting the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 (1-888-743-0023) or by visiting its website at www.oag.state.md.us.

Please be assured that we take the protection of your information very seriously. We regret any inconvenience or concern this incident may cause you.

Sincerely,

Deborah L. Johnson
Chief Human Resources Officer,
On behalf of Pillsbury Winthrop Shaw Pittman LLP

Enclosures

ID TheftSmart™

<First Name> <Middle Initial> <Last Name> <Suffix>
Membership Number: <Membership Number>

Member Services: 1-800-XXX-XXXX
 8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday
 If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services

ID TheftSmart™

<First Name> <Middle Initial> <Last Name> <Suffix>
Membership Number: <Membership Number>

Member Services: 1-800-XXX-XXXX
 8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday
 If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services

Please detach cards and keep in a convenient place for your reference

**Pillsbury Winthrop Shaw Pittman LLP
Security Breach FAQ's
July 2008**

Q1: What is this about?

A1: On Memorial Day (May 26, 2008), there was a break-in and theft of computers at Colt Express Outsourcing Services, Inc. ("Colt"), which is a company that Pillsbury hired to handle benefits plan billing in 1998, and COBRA administration from mid-1998 to mid-2002. The computers that were stolen contained information about Pillsbury employees including their name, address, social security number, date of birth, names of dependents and dependent social security numbers. The information included employees who had worked for Pillsbury between 1998 and 2002. Pillsbury found out about this theft on about June 16, 2008, when we received a letter from Colt describing the incident. We terminated our relationship with Colt in 2002.

Q2: What is Pillsbury doing?

A2: Pillsbury has been working diligently to determine what information and which individuals may have been affected. We have taken additional measures to protect information regarding you that we maintain, and we are also working with our past and current vendors to fortify security practices already in place to prevent future potential security breaches.

As a precaution, Pillsbury is providing notification to people whose information may have been in the databases so that if it turns out the information was compromised in any way, they can take appropriate action to protect themselves.

Pillsbury is also providing access to Kroll Inc.'s ID TheftSmart™ service through July 2009. This service includes Continuous Credit Monitoring and a Trimerged Credit Report at no cost to you. Should you suspect that you may be a victim of identity fraud, you will have access to Kroll's Licensed Investigators for guidance and consultation.

Colt has already reported the theft to the Walnut Creek Police Department and is cooperating in the investigation with law enforcement.

Q3: What information was on the computers that were stolen?

A3: The computers contained name, address, social security number, date of birth and dependent information. It is not clear whether the thief was able to access the information on the computers.

Q4: Was health information exposed?

A4: No.

Q5: Were credit card numbers exposed?

A5: No.

Q6: Were bank account numbers exposed?

A6: No.

Q7: Were driver's license numbers exposed?

A7: No.

Q8: If my information was in the file, what should I do?

A8: If you received a letter from Pillsbury, then your name was in one of the files that was on one of the computers. Your social security number may have been in that file.

You can enroll in Kroll's ID TheftSmart service. Information about this service is enclosed. This service includes Continuous Credit Monitoring and a Trimerged Credit Report through July 2009, at no cost to you. Should you suspect that you may be a victim of identity fraud, you will have access to Kroll's Licensed Investigators for guidance and consultation.

Q9: How do I enroll in Kroll's ID TheftSmart service?

A9: Complete and return the enclosed authorization form as soon as possible. If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services at 1-500-XXX-XXXX between 8:00 a.m. and 5:00 p.m. (Central Time), Monday through Friday. Unfortunately this service is not available for minors or decedents.

Q10: What else can I do?

A10: You can also contact one of the three credit reporting bureaus and place a 90-day Initial Fraud Alert on your credit file. That bureau will notify the other two bureaus and will send you confirmation that the alert has been placed along with a free copy of your credit report. Review your credit report carefully to see if there has been any new credit requested. Mark on your calendar to review all this information again every four months. Sometimes identity thieves will wait for time to pass before using your information.

Q11: How will I know if my information was used by someone else?

A11: The best way to find out is to get a copy of your credit report from one of the three credit reporting bureaus. The credit report will show if there has been any new credit requested using your information.

Q12: How do I put a Fraud Alert on my credit report?

A12: US law allows you to put a "fraud alert" on your credit report. This is a free service. A 90-day Initial Fraud Alert puts a statement on your credit file that you may have been or are about to become the victim of identity theft or other fraud. If you specify a telephone number, anyone using your credit report must call that number or take reasonable steps to verify your identity to confirm that a credit application is not the result of identity theft.

After you put a fraud alert on your credit report, you will be asked to provide proof of your identification when you apply for credit. This may limit your ability to apply for instant credit for in-store purchases but it should not interfere with your daily use of existing credit cards or banking accounts.

You can put a 90-day Initial Alert on your credit report by contacting one of the three major credit bureaus. The one you contact will notify the others. This will entitle you to a free credit report. You will receive confirmation of the alert from the bureau you contact. At the end of the 90 day period you may place an additional Initial Fraud Alert on your credit file. We suggest that you do this every 90 days for at least one year.

Q13: How can I get in touch with the credit bureaus?

A13: There are three major credit bureaus. They are:

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

Equifax
800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241

Trans Union
800-680-7289
Fraud Victim Assistance Div.
P.O. Box 6790
Fullerton, CA 92834-6790

Q14: Do I have to pay for a credit report?

A14: You are entitled to one free credit report a year from each of the three credit reporting bureaus. This means that you can receive one today from one (e.g. Experian), you can receive another in four months (e.g. from Equifax), and you can receive another in eight months (e.g. from TransUnion). By spacing out your requests for your free credit report you can monitor your credit over the course of a year. If you want to receive more than one credit report from any of the credit reporting bureaus during the same year, you may have to pay a small charge.

Q15: How long will it take to get my credit report?

A15: You can access your credit report online at www.annualcreditreport.com. You can download or print the report from that site. You may also request the report by telephone (by calling 1-877-322-8228 and answering some questions to verify who you are) or by mail (by downloading the request form from www.annualcreditreport.com and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281). If you request your report by phone or by mail it will take approximately two weeks to process the request, so you should allow two to three weeks for delivery to you.

Q16: What is a fraud alert?

A16: A fraud alert is a message added to your credit report that tells anyone who pulls a copy of your credit report telling them that there is possible fraud associated with your account. It gives them a telephone number to call you before issuing any new credit. A 90-day Initial Fraud Alert expires after 90 days. If you have been the victim of identity theft you may be able to place a 7-year fraud alert on your account. You can obtain more information online at <http://www.consumer.gov/idtheft>.

Q17: How long does a fraud alert last?

A17: The Initial Fraud Alert lasts 90 days after it is placed on your report. You can remove the alert by calling the credit bureaus before the 90 days expires. You can place an initial alert every 90 days by calling one of the credit bureaus.

Q18: Will a fraud alert stop me from using my credit cards?

A18: No. However, a fraud alert may interfere with your ability to get immediate credit, for instance if you apply for instant credit at a department store. This is because the department store credit office will have to call you to verify your identity before issuing you credit.

Q19: Can I still apply for credit if I put a fraud alert on my credit report?

A19: Yes. The fraud alert may slow down the process of getting approval for credit because the fraud alert will require that the creditor verify your identity before approving new credit.

Q20: What should I watch out for on my credit report?

A20: Look for any accounts that you don't recognize especially new accounts. Look in the personal information section to see if the residence and employment information is correct or has changed. These things could be indications of fraud. If you see information you do not understand or that is wrong, call the credit bureau at the number on the report and speak to a staff member. If the information cannot be explained, contact your local police or sheriff's office.

Q21: If someone has used my information, what should I do?

A21: You should immediately notify your local police or sheriff's office and file a report. Get a copy of the police report, because you may need to give a copy to the credit bureaus or creditors. Also contact one of the three credit bureaus and place a fraud alert on your account. For more information you can visit the website: www.consumer.gov/idtheft.

Q22: Do I have to call all three credit bureaus?

A22: When you call one bureau, it will pass the report on to the other two. You should receive a confirming letter from each of the three bureaus. If you do not receive confirmations from all three credit bureaus, call the bureau which did not confirm the alert.

Q23: Will anyone contact me to ask for my personal information because of this event?

A23: No. Pillsbury will not contact you unless you call or write to us first. We will never ask for your social security number. If you are contacted directly by someone who claims to be with Pillsbury and who asks you for your personal information, please immediately contact us and your local sheriff's office to report the suspicious contact.

Q24: I have been contacted directly by someone claiming to be from Pillsbury or a law enforcement agency asking for my personal information (e.g., social security number, etc.). Did you contact me? What should I do?

A24: No. We did not contact you unless you called or wrote us first. We would never have asked for your social security number. If you were contacted directly by someone who claimed to be with Pillsbury or law enforcement and who asks you for your personal information, please immediately contact us and your local sheriff's office to report the suspicious contact. You may also provide us with your name and telephone number and we will have the appropriate authorities contact you directly. When law enforcement contacts you, they will reference your contact with Pillsbury.

HELPFUL WEBSITES

Credit Reporting Bureaus:

Annual Credit Reports: <http://www.annualcreditreport.com>

Experian

<http://www.experian.com>

888-397-3742

P.O. Box 2002

Allen, TX 75013

Equifax

<http://www.equifax.com>

800-525-6285

P.O. Box 740241

Atlanta, GA 30374-0241

TransUnion

<http://www.transunion.com>

800-680-7289

Fraud Victim Assistance Division

P.O. Box 6790

Fullerton, CA 92834-6790

Federal Trade Commission

Identity Theft

<http://www.consumer.gov/idtheft>

Hotline: 877-ID-THEFT (877-438-4338)

affidavit: <http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>

Filing a Complaint with the FTC

<http://www.ftc.gov>

1-877-FTC-HELP (1-877-382-4357) (TTY: 1-866-653-4261)

Social Security Administration

<http://www.ssa.gov>

Fraud Hotline: 800-269-0271

Benefits Statement: 800-772-1213

Privacy Rights Clearing House Identity Theft Resources

<http://www.privacyrights.org/identity.htm>

This not-for-profit organization provides statistics, fact sheets and government records about identity theft.

Identity Theft Resource Center

<http://wwwidtheftcenter.org>

This not-for-profit organization is dedicated exclusively to identity theft. It provides consumer and victim support about identity theft and includes resources, consumer alerts and instructions for victims.