

**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: Zhone Technologies, Inc.
Address: 7001 Oakport Street
Oakland, CA 94621
Telephone: 510-777-7000
Fax: 510-777-7001
Email: LLarsen@zhone.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 9, 2008
Date the Security Breach was discovered: The theft occurred on May 26, 2008 and was discovered by Colt on May 27, 2008, but Zhone did not receive notice of the breach until June 9, 2008.
Estimated number of affected individuals: Approximately 3,000 Zhone employees, former employees and dependents
Estimated number of NC residents affected: 42

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, Suite 210, Walnut, Creek, CA 94598, 1-800-265-8397, www.ColtHR.com

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: Zhone was told that the offices of Colt were burglarized on May 26, 2008 and certain computers were stolen. The computers may have contained the personally-identifying information of Zhone employees. This information was in electronic format.

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. ^{Zhone was told that the information was not encrypted} If so, please describe the security measures protecting the information: We have been unable to determine whether it was password protected.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: We have been unable to obtain this information from Colt. Colt is a former vendor. Colt's contract with Zhone ended over a year ago. Colt apparently retained Zhone's data on Colt's computers even though Colt's contract with Zhone had long since ended. Zhone has demanded that Colt return or destroy any of Zhone's data still in Colt's possession.

Date affected NC residents were/will be notified: June 16, 1008

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): N/A

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: _____ Date: _____
Contact Person, Title: _____
Address: _____
(if different from above) _____
Telephone: _____ Fax: _____ Email: _____



people. process. profit.

June 4, 2008

LAURA LARSEN
ZHONE TECHNOLOGIES, INC.
7001 OAKPORT STREET
OAKLAND, CA 94621-

Re: Notice of Potential Data Security Breach on May 26, 2008

Dear LAURA LARSEN,

Colt Express Outsourcing Services, Inc. ("Colt Express"), previously provided your company benefit plan administration services. We write to notify you of a potential data security breach involving the personal information of some of your current and former employees and their dependents during the time period of 01-Sep-03 to 01-Jun-07.

Enclosure 1 is a breakdown by state of the total number of your current or former employees and their dependents who could be affected by this incident.

The breach occurred on Memorial Day, Monday, May 26, 2008, between approximately 4:30 p.m. and 5:00 p.m. PST, when someone broke into Colt Express's office at 2125 Oak Grove Road, Suite 210, Walnut Creek, California, 94598

Upon discovery the next morning, the break in and theft were reported immediately to the Walnut Creek Police Department, report number 08-12367. Subsequently, Colt Express has followed up with Walnut Creek PD and the REACT High Tech Crimes Task Force in Silicon Valley. Colt Express will continue to follow up and work with law enforcement about the incident. At this time, we do not know if personal data has been accessed or misused.

We understand that you will need to notify your current and former employees, whose information may have been exposed, about this incident. Kroll, Inc., a leading risk consulting company that provides data breach response services, informs us that even though employer companies have a reasonable time in which to notify, they too often react too quickly and notify their employees before a plan is in place to ensure an orderly response process. Thus creating unnecessary, additional consternation among affected individuals. Kroll, Inc., encourages that the notification be made properly as opposed to quickly, and after a sound solution and response plan is in place and ready to execute.

We will send you the data which may have been compromised in an Excel format. When you are ready to receive it, have the authorized individual send an email from your company's domain to us at datarequest@colthr.com with the following text in the subject line: "Data Request." Colt Express will then "reply" to that address using Tumbleweed's Secure Messaging product. The "reply" recipient will first receive an email notification from us. By pressing the button "view report" on the email, the recipient will be directed to our secure server and will be able to download your file with SSL protection. Once you receive the data from us, you should feel free to verify that the employee information that we have that you provided to us is consistent with your information.

As a courtesy, Enclosure 2 is a "Sample Individual Notification Letter" containing information about the incident. Some states have different content requirements for individual notification letters. We do not represent that this letter meets all of those state requirements. Therefore, do not simply use this letter; you should consult with legal counsel for the appropriate content for your individual letters by state. You may want to engage a company that provides comprehensive data breach response services, such as written notification to the affected individuals; credit reports and monitoring; fraud investigation; and restoration services. Such companies can ensure an orderly and proper individual notification process that greatly reduces the stress and anxiety often associated with such data breach incidents.

For your convenience, Enclosure 3 provides information about Kroll, Inc., the risk consulting company mentioned above, and the data breach response services it provides. You should, of course, choose the company you wish to work with. We enclose Kroll, Inc.'s information only out of courtesy and to give you an idea of the types of services available.

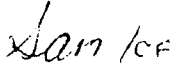
Some states may require your company to send written notification of this data security breach incident to their particular state regulatory agencies or credit bureaus. Again, you should consult with legal counsel to determine which states require such written notification and the appropriate content of such notification.

Colt Express takes the protection of its customer and personal information very seriously. Colt Express is taking steps to ensure that a potential data security breach does not occur in the future. We installed an alarm system Friday, May 30th. Colt Express is looking into what additional steps may be taken to provide enhanced security.

By this letter and enclosures, we are providing you with all the information we believe you need, and that we are able to give you. We do not have the resources, financial and otherwise, to assist you further. Towards the end of last year, our customer base was reduced to an unsustainable level. Colt has been in the process of going out of business, while at the same time providing time for remaining customers to find alternative solutions. Those decisions are now final.

We are firmly committed to protecting all of the information that is entrusted to us both before and after we close down. We sincerely apologize for the inconvenience and concern this incident will cause. When you have any additional questions about this incident, please call me at (925) 927-5440. I will respond to your call just as soon as I am able to do so.

Sincerely,



Samuel G. Colt III
Chief Executive Officer
Colt Express Outsourcing Services, Inc.
Encls.

ZHONE TECHNOLOGIES, INC.

| State | Employees | Dependents |
|-------|-----------|------------|
| AL | 1 | 0 |
| AZ | 2 | 2 |
| CA | 426 | 659 |
| CO | 12 | 18 |
| CT | 4 | 9 |
| FL | 342 | 483 |
| GA | 40 | 85 |
| HI | 1 | 0 |
| IL | 8 | 17 |
| IN | 1 | 1 |
| KS | 1 | 3 |
| KY | 1 | 4 |
| MA | 16 | 39 |
| MD | 1 | 4 |
| ME | 4 | 12 |
| MI | 1 | 0 |
| MN | 4 | 8 |
| MS | 1 | 6 |
| MT | 2 | 6 |
| NC | 11 | 31 |
| ND | 1 | 1 |
| NH | 28 | 55 |
| NJ | 144 | 238 |
| NV | 3 | 5 |
| NY | 7 | 14 |
| OK | 3 | 7 |
| OR | 8 | 14 |
| PA | 5 | 6 |
| RI | 1 | 4 |
| SC | 1 | 1 |
| TX | 18 | 42 |
| VA | 13 | 18 |
| WA | 4 | 10 |
| WI | 3 | 7 |
| other | 2 | 2 |

Exhibit 2: Sample Individual Notification Letter

<First Name> <Middle Initial> <Last Name> <Suffix>
<Address> (Line 1)
<Address> (Line 2)
<City> <State> <Zip>

Dear <First Name> <Middle Initial> <Last Name> <Suffix>,

We are writing to let you know that your personal information, including name, address and Social Security number, may have been subject to unauthorized access or acquisition as a result of a break in and theft of computers at the offices of one of our external benefit administration vendors. If we provide or have provided benefits to your dependents, their personal information may have also been exposed by this incident. Even though we do not know whether your personal information has been accessed or misused, we want to make you aware of the incident and the steps <we have taken> <you should take> to guard against identity fraud.

To safeguard yourself against identity theft or other unauthorized use of personal information, you can take some simple steps. First, we recommend that you remain vigilant over the next 12 months and review your credit card bills and credit report for unauthorized activity. You should also promptly report any suspected identity theft of fraud to your local law enforcement agency, the U.S. Federal Trade Commission, your financial institution, and to the Fraud Alert phone line of one of the three national consumer reporting agencies by calling: Experian 1-888-397-3742; Equifax 1-800-525-6285; or TransUnion 1-800-680-7289. You may obtain a 90 day Fraud Alert status on your record by calling one of the credit bureau phone numbers.

You have the right to obtain a police report if you are the victim of identity theft. You may wish to contact your credit card issuers and financial institutions and inform them of the incident as well.

In addition, you may contact the fraud departments of the three national consumer reporting agencies to discuss your options. You have the right to place security freeze on your consumer report. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent; however, please be aware that using a security freeze may delay your ability to obtain credit. You may request that a security freeze be placed on your consumer report by sending a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail to the address below. The following information should be included when requesting a security freeze (please note that if you are requesting a credit report for your spouse or other dependent,

Exhibit 3: Kroll Services Information

Kroll Inc., the world's leading risk consulting company, provides a broad range of investigative, intelligence, financial, security and technology services to help clients reduce risks, solve problems, and capitalize on opportunities.

- Since its founding in 1972, Kroll has continuously expanded the breadth and depth of its risk management services and served an elite clientele consisting of the world's leading multinational corporations, non-profit institutions, and government agencies.
- Kroll's identity theft solutions are the culmination of years of practical experience. Kroll and its licensed investigators have been working with organizations and consumers to uncover and resolve identity theft issues since 1999.
- Kroll's licensed investigators are highly trained and experienced in identity theft restoration issues. Since 1999, they have counseled and provided representation for millions of individuals. Kroll assigns each victim a licensed investigator who does the restoration work on their behalf.
- Kroll provides a comprehensive plan with various benefit options that can be tailored to meet our client's needs.

Kroll's services include access to:

- Preventative and investigative consulting services
 - Forensic investigative services
 - Notification and enrollment of affected consumer groups
 - Call triage center to manage consumer expectations
 - Credit reports, with analysis and credit monitoring
 - Non-credit services for affected consumers without access to credit reports or monitoring
 - Identity theft investigative services
 - An identity restoration and consulting call center
- Kroll Background America, Inc. (KBA), the subsidiary through which Kroll offers identity theft services, is one of the few companies in the United States that is Safe Harbor compliant and thus able to address the security requirements of the European Union's Data Protection Act. KBA has established processes and procedures with credit repositories and government agencies and complies with the Fair Credit Reporting Act and other applicable regulations.

exist in the consumer's name. Following the investigation, should Identity theft exist, Kroll will prepare and forward a restoration case review document for your review. The vast majority of ID Theft issues are not discovered through credit reports or through credit monitoring, examples include rental housing fraud, utilities fraud, health benefits fraud, W-2 fraud, check fraud and a host of other non-credit activity.

- 4. Restoration Services:** *Upon your review and approval to work a case*, Kroll will manage, drive and facilitate comprehensive restoration services on behalf of the victim. Kroll can assist the victim with obtaining a police report as a prerequisite to work a case on a victim's behalf and retains a "limited power of attorney" enabling Kroll investigators the legal right to resolve issues for them. Kroll investigators are well versed in dealing with even the most unusual cases. Our team knows what to do, who to call and who to utilize if we do not receive the results according to a victims rights. This can involve an Attorney General, Office of Thrift Supervision, US Postal Inspector, etc...

Restoration Services; If an enrolled member has an Identity Theft issue that you believe is attributed to your breach of data, Kroll will open a case and work it until those issues that can be resolved, are. An unfortunate truth about the work we do is that some issues cannot be resolved, should a victim get placed on the "OFAC no fly list", we cannot guarantee removal.

Should you believe an ID Theft issue is not due to your breach of data; Kroll can provide restoration services to the member for the same discounted rate.

- 5. Non Credit Response:** Kroll provides a standard package of services to consumers or employees affected by a data loss event. In cases where those affected by the event are unable to receive credit services i.e. **deceased, minors, expatriates and foreign nationals**, Kroll provides enrollment, notification, call center access, investigative services and restoration services to address the unique needs of this stakeholder group. All services listed above sans credit services are provided to this stakeholder group with the understanding that certain privacy issues may impede the progress of the investigator and require the victim of identity theft to become more involved in the restoration process.
- 6. Address Verification:** Should your event contain historical or aged data, Kroll can investigate the affected consumer to discern their most recent mailing address. This service has proven beneficial when proving "best effort" to notify affected consumers under various State and privacy statutes.

Zhone Technologies, Inc.

@ Zhone Way
7001 Oakport Street
Oakland, CA 94621
Phone: 510.777.7000
Fax: 510.777.7001

www.zhone.com



Z H O N E .

June 16, 2008

Dear :

We are writing to you because of a recent security incident on the part of one of our third party service providers. We are informed that on May 26, 2008 the office of our third party service providers was burglarized and certain computers were stolen. These computers may have potentially contained your personal information, including name, address, birthday, last hire date, last billing date and Social Security number. If we provide or have provided benefits to your dependents, their personal information may have also been impacted by this incident. We do not know whether your personal information in fact has been accessed or misused; however, we want to make you aware of the incident and the steps Zhone Technologies, Inc. ("Zhone") has taken to help you and give you suggestions on how to guard against security fraud.

Zhone has engaged ConsumerInfo.com, Inc., an Experian® company, to provide you with one full year of credit monitoring, at no cost to you. This credit monitoring product known as Triple AdvantageSM Premium will identify and notify you of key changes that are detected on any of your credit reports from the three credit reporting companies: Experian, Equifax® and TransUnion®. This credit monitoring product is a powerful tool that you can use to help you identify possible fraudulent use of your information.

Your complimentary 12-month Triple AdvantageSM Premium membership includes:

- One, free 3-Bureau Credit Report and Score upon enrollment
- Daily monitoring of your three credit reports from Experian, Equifax® and TransUnion®
- Email alerts if key changes are detected on any of your three credit reports
- Monthly "No Hit" alerts, if applicable
- Toll-free access to a dedicated team of Fraud Resolution Representatives if you should detect any fraudulent activity on your credit report or become a victim of identity fraud
- \$25,000 in identity theft insurance provided by Virginia Surety Company, Inc. with no deductible*

*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York.

You have ninety (90) days to activate this membership, which will then continue for 12 full months. We encourage you to activate your credit monitoring membership as soon as possible.

- To sign up online, please visit <http://partner.consumerinfo.com/zhone> and enter your individual activation code provided below. Please keep in mind that once activated the code cannot be re-used. You will be instructed on how to enroll in your complimentary credit monitoring product. If you sign up online, all credit reports and alerts will be delivered via email.
- To sign up by telephone, dial 866-252-0121. If you sign up by telephone, all credit reports and alerts will be delivered via U.S mail.

Your Single Use Credit Monitoring Activation Code: [ZHT438HHE]

In addition, there are some simple steps that you may take to safeguard yourself against identity theft or other unauthorized use of your personal information:

- Remain vigilant over the next 12 months and review your credit card bills and credit report for unauthorized activity.
- Promptly report any suspected identity theft or fraud to your local law enforcement agency, the U.S. Federal Trade Commission and your state attorney general. You can call the U.S. Federal Trade Commission at 1-877-FTC-HELP (1-877-382-4357) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. The following website lists the names, telephone numbers and addresses of the state attorney generals: http://www.naag.org/ag/full_ag_table.php. You can also obtain additional information from these sources about additional steps you can take to avoid identity theft.
- Promptly report any suspected identity theft or fraud to your financial institution, and to the Fraud Alert phone line of one of the three national consumer reporting companies by calling: Experian 1-888-397-3742; Equifax 1-800-525-6285; or TransUnion 1-800-680-7289.
- Contact the fraud departments of the three national consumer reporting companies to discuss your options, including obtaining a 90 day Fraud Alert status on your record.
- You have the right to obtain a police report if you are the victim of identity theft. You may wish to contact your credit card issuers and financial institutions and inform them of the incident as well.
- Place a security freeze on your consumer report. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent; however, please be aware that using a security freeze may delay your ability to obtain credit. You may request that a security freeze be placed on your consumer report by sending a request to a consumer reporting company by certified mail, overnight mail or regular stamped mail to the addresses below. The following information should be included when requesting a security freeze: (a) name; (b) address; (c) date of birth; (d) social security number; (e) proof of current address such as a current utility bill; (f) payment of applicable fees to request a security freeze of your credit file.¹

¹ Most agencies accept personal checks, American Express, Mastercard, VISA, and Discover Cards for payment of fees. Please call each at the numbers provided above to determine the fee for your state and what forms of payment are accepted. If you are paying by credit card, please include the following information: (a) name of the person as it appears on the credit card; (b) type of credit card (American Express, Mastercard, VISA, or Discover Card); (c) complete account number; (d) expiration date (month and year); (e) for American Express - 4 digit Card Identification Number (on front of card above the account number); and (f) for Mastercard, VISA, or Discover Card - 3 digit Card Identification Number (on back of card at the end of the account number). Please do not send cash through the mail.

- Include a copy of a police report, Identity Theft report, or other government law enforcement agency report, such as a DMV report if you are an identity theft victim and are requesting a security freeze you must also.

Send your requests to the following addresses:

(1) Equifax

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348

(2) TransUnion

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

TransUnion
Fraud Victim Assistance Department
1561 E. Orangethorpe Ave.
Fullerton, CA 92831

(Use this address only if you are a New York, New Jersey, and West Virginia resident who is making your request to TransUnion via overnight mail. All other individuals should make their request to the address above.)

(3) Experian

The address for Experian varies depending on your state of residence and the manner in which you send your request (e.g.: overnight mail, regular mail, certified mail, etc.). Please call Experian at 1 888 EXPERIAN (1 888 397 3742) or visit Experian's website at the following URL and select your state of residence to find the appropriate address:
http://www.experian.com/consumer/security_freeze.html.

To find out more information about security freezes and each agency's particular requirements, visit the agency websites located at:

(1) Equifax:

http://www.equifax.com/cs/Satellite?c=EFX_ContentRoot&cid=1165203975981&pagename=5-1%2F5-1_Layout

(2) TransUnion

<http://www.transunion.com/corporate/personal/fraudIdentityTheft/preventing/securityFreeze.page>

(3) Experian

http://www.experian.com/consumer/security_freeze.html.

Please accept our sincerest apologies for any inconvenience that may be caused by this notice.

Rest assured, we have stopped using the third party Service provider. We are committed to fully protecting all of the information that is entrusted to us. If you have any additional questions about this incident, please contact Zhone at: Laura Larson, Director, Human Resources & Administration, Zhone Technologies, Inc., 7001 Oakport St. Oakland, Ca 94621; Telephone: 510-777-7062; fax: 510-777-7359.

Sincerely,

A handwritten signature in cursive script that reads "Laura Larson".

Laura Larsen

Director, Human Resources