

WHITEFORD, TAYLOR & PRESTON L.L.P.

SEVEN SAINT PAUL STREET
BALTIMORE, MAINE 21202-1636
MAIN TELEPHONE (410) 347-8700
FACSIMILE (410) 752-7092

BALTIMORE, MD
COLUMBIA, MD
FALLS CHURCH, VA
TOWSON, MD
WASHINGTON, DC
WILMINGTON, DE*

WWW.WTPLAW.COM
(800) 987-8705

LELAND C. MOORE, JR.
COUNSEL
DIRECT LINE (410) 347-9413
DIRECT FAX (410) 223-4303
LMoore@wtplaw.com

June 3, 2010

Via Federal Express

Attorney General Janet T. Mills
6 State House Station
Augusta, ME 04333
Attn: Security Breach Notification

CONSUMER PROTECTION DIVISION
RECEIVED

JUN 4 2010

OFFICE OF ATTORNEY GENERAL

Dear Sir/Madam:

For and on behalf of our client, Integrity Applications Incorporated ("IAI"), a Virginia corporation located at 5160 Parkstone Drive, Suite 230, Chantilly, VA 20151, we are writing to inform you of an incident involving the theft of a laptop computer from IAI which contained the personal information of one (1) Maine resident.

The IAI computer was stolen on May 12, 2010 in Fairfax County, Virginia. The theft was reported to local law enforcement. IAI was informed of the theft the next day and immediately took steps to secure IAI's network and information systems to prevent unauthorized access. Simultaneously, IAI commenced an internal investigation to determine, as accurately as possible, the types of information stored on the computer, the level of security protecting the information and the identity and residency of the persons whose personal information may be on the computer.

IAI has been diligently investigating this incident and has now determined that on the computer is an electronic database containing information regarding certain individuals associated or formerly associated with IAI, including personal information such as, name, social security number and date of birth, and other information related to the individuals' assignments at IAI. IAI has identified those individuals whose personal information is in the database. The computer does not contain any bank account, credit card or other financial account information. Both the computer and the database were password-protected and also require a non-apparent, valid user name to gain entry to the computer and database. As of the date of this letter, IAI is not aware

of and has not received any reports of identity theft, fraud or other misuse of the personal information on the computer.

In addition to the responsive measures described above, IAI is preparing to send written notification to the single Maine resident who may be affected by this incident. A copy of the form of notification to the Maine resident is attached to this letter. IAI presently plans to notify this resident by letter on or about June 4, 2010.


To help protect the individuals whose personal information was contained on the computer from the possibility of identity theft and/or fraud, IAI has purchased a full-year of identity theft protection from LifeLock, Inc., for each individual affected, at IAI's expense. IAI has also undertaken a full review of its information security policies, procedures and practices and is committed to making improvements wherever necessary to help protect the personal information in IAI's possession and to avoid a recurrence of this incident.

Please be assured that IAI takes information security very seriously and is committed to protecting the confidentiality of the personal information in its possession. IAI regrets that this incident occurred and will continue its efforts to avoid any recurrence of this type of incident in the future.

If you have any questions about this incident or the proposed notification to the resident, please contact me directly at (410) 347-9413.

Sincerely,

WHITEFORD, TAYLOR & PRESTON, LLP

By: 
Leland C. Moore, Jr.
Counsel
*On Behalf of Integrity Applications
Incorporated*

Enclosures

[Date]

[Resident Name]
[Address]
[City, State, Zip Code]

Dear [Resident Name]:

We are writing to notify you of the theft of an IAI-owned laptop computer that may contain certain of your personal information and to inform you of the actions we have taken to help protect you, and that you may take to protect yourself, against any risks of identity theft, fraud or other misuse of your personal information. We sincerely apologize for any inconvenience this incident may cause you and thank you for your understanding and cooperation as we continue our investigation.

On May 13, 2010, IAI learned that a company-owned laptop computer had been stolen during the prior evening, on May 12, 2010, in Fairfax County, Virginia. The theft of the laptop was reported to local police within hours of the theft. When IAI learned of the theft, we immediately took action to secure our systems and began investigating to determine the contents of the stolen laptop. Our investigation has now determined that the laptop likely contained information pertaining to certain individuals associated or formerly associated with IAI, including personal information such as name, social security number, and date of birth and other information related to IAI assignments. The laptop and the database containing the personal information were both password-protected. The information on the laptop did not include any bank account, credit card or any other financial account information.

We are notifying everyone who might possibly be affected by this incident even while our investigation is continuing to help protect against any risk of identity theft, fraud or other mischief involving your personal information. We believe the information on the laptop is not easily accessed nor readily usable due to the password protection and the database format and, as of the date of this letter, we are not aware of and have not had any reports of identity theft, fraud or other misuse of the information on the laptop.

As soon as we learned of the theft, we took immediate action to ensure that no further information was at risk and we immediately implemented heightened enforcement of our information security policies. We will also be undertaking a full review of those policies to identify any areas that might be improved going forward. By your association with IAI you know firsthand that we take information security very seriously and we have undertaken a full review of our information security policies, procedures and practices to prevent a recurrence of this type of incident.

Identity Theft Protection Arranged by IAI

To help protect you from the possibility of identity theft and/or fraud as a result of this incident, IAI has engaged **LifeLock, Inc.** (www.lifelock.com), an identity theft protection firm, to provide you with a full year of identity theft protection services at IAI's expense. The enclosed **LifeLock** brochure describes the benefits and services included with your membership, once you have completed your enrollment. We believe the **LifeLock** service will provide you with a considerable measure of protection and we hope you will take advantage of it.

To enroll and begin utilizing **LifeLock's** services immediately:

- Call 1-877-509-5357 or visit www.lifelock.com to enroll.
- Use this promotion code: **INTEGRITYEMP**, when prompted, as well as your Member ID.
- Your Member ID is **XXXXXX**. This Member ID is unique to you and should not be shared with others.
- LifeLock's specialized team of telephone representatives are available 24 hours a day, seven days a week to answer any questions you may have regarding the recent data breach.
- You must enroll within 60 days of this letter.
- If you are already a member of **LifeLock**, IAI will extend your current membership through June, 2011.

Additional Steps To Take To Help Protect Against Identity Theft

We also recommend that you take other steps to protect yourself from the possibility of fraud and identity theft and remain vigilant by monitoring your account statements and free credit reports for unexplained, suspicious or unauthorized activity.. You may obtain a copy of your credit report once per year, free of charge, whether or not you suspect any unauthorized activity on your account, by contacting each of the nationwide consumer credit reporting agencies identified below, or by visiting www.annualcreditreport.com. You may obtain information about additional protections, such as fraud alerts and security freezes, from each of the three credit reporting agencies shown below. For your convenience, general information about requesting a security freeze is enclosed with this letter.

Equifax
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30348
www.equifax.com

Experian
(888) 397-3742
P.O. Box 2104
Allen, TX 75013
www.experian.com

TransUnion
(800) 916-8800
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com

The Federal Trade Commission (FTC) recommends that you check your credit reports periodically to help you spot problems and address them quickly. If a report shows accounts you did not open, inquiries from creditors that you did not initiate, personal information, such as a home address, that is inaccurate, or other information you do not understand, contact one of the credit reporting agencies immediately. In addition, if you find suspicious activity on your credit reports or have reason to believe your personal information is being misused, authorities generally recommend that you take two additional steps: First, call your local law enforcement agency and file a police report. Get a copy of the report as many creditors want the information it contains to absolve you of any fraudulent charges. Second, file a complaint with the FTC, which will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement agencies for their investigations.

You can file a complaint or obtain additional information about preventing identity theft from the Federal Trade Commission:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
(877) 438-4338

How To Reach IAI For Additional Information About This Incident

To answer any questions or address any concerns you may have, we have set up a toll-free telephone number for you to call during regular business hours:

1-877-504-4424 Ext. 294

If you are a resident of Maryland or North Carolina, please see the following page for additional information applicable to you.

IAI regrets that this incident occurred and is taking swift action to avoid a recurrence. Again, on behalf of the entire management team, I sincerely apologize for any inconvenience this incident may cause you.

Sincerely,

Joseph L. Brickey
Chairman and CEO

Special Notice For Maryland Residents:

The Maryland Office of the Attorney General and the Federal Trade Commission (FTC) can provide you with additional information about steps you can take to avoid identity theft and may be contacted at:

Maryland Office of the Attorney General
Consumer Protection Division
200 Saint Paul Place
Baltimore, Maryland 21202
Toll free: (888) 743-0023
www.oag.state.md.us/idtheft/

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
Toll free: (877) 438-4338
www.ftc.gov/idtheft

Special Notice For North Carolina Residents:

The North Carolina Attorney General's Office and the Federal Trade Commission (FTC) can provide you with additional information about steps you can take to avoid identity theft and may be contacted at:

North Carolina Attorney General Ray Cooper
P.O. Box 629
Raleigh, NC 27602
(919) 716-6400
Toll free: (877) 566-7226
www.ncdoj.com

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Toll free: (877) 438-4338
www.ftc.gov/idtheft

HOW TO REQUEST A SECURITY FREEZE

Following is general information about how to request a security freeze from the three credit reporting agencies. While this information is believed to be accurate, you should contact each agency for the most accurate and up-to-date information.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. In some states, if you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Trans Union Security Freeze Fraud Victim Assistance Department P.O. Box 6790 Fullerton, CA 92834
--	---	---

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.