Wentworth
Institute of Technology

February 4, 2011

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Delaney:

We are writing to notify you of an unauthorized access of personal information involving 88 New Hampshire residents.

NATURE OF THE UNAUTHORIZED USE OR ACCESS

Wentworth received an email at 9:00 PM on Monday, December 20, 2010, informing us that there was confidential personal information available in a file on the Institute's website. Some files originally created for Wentworth Opening Week (our official welcome program for all incoming first-year and transfer students) in 2003, 2004 and 2005 (most of the information was from 2003) were originally located on a secure web server, where the files were secure from unauthorized access. On April 10, 2007, the files were moved to a non-secure web server, where they were no longer secure from unauthorized access.

For all of the affected individuals (including 88 New Hampshire residents) the confidential personal information included in the files was name, date of birth and social security number. For some of the affected individuals (including 31 New Hampshire residents) the information also included allergies, medications, medical conditions, and disabilities that the individual had provided to Wentworth in connection with his/her registration for Wentworth Opening Week.

The information was all in electronic form.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Because the address information in our records for the affected individuals was over seven years old in some cases, we contracted with MacDonald Information Service, Inc. to provide current addresses for affected individuals. Based on the information provided by MacDonald and comparison with our own student records, we have determined that the list of affected individuals included 8 Maryland residents.

We have notified all affected individuals identified as New Hampshire residents by first-class U.S. mail. These individual notifications were mailed on January 14, 2011.

New Hampshire residents received one of two letters depending on whether or not the information that was publicly accessible included information such as allergies, medications, medical conditions, and disabilities that the individual had provided to Wentworth in connection with his/her registration for Wentworth Opening Week. Copies of both letters are enclosed.

550 Huntington Avenue • Boston, Massachusetts 02115-5998 • (617) 989-4590 • Fax (617) 989-4591
www.wit.edu

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

Immediate Incident Response

Wentworth was informed by e-mail of unauthorized access of confidential data on a Wentworth public facing server the evening of December 20, 2010. The e-mail was forwarded to Wentworth's Division of Technology Services (DTS) the next morning. Immediately upon notification, DTS confirmed the presence of the files on a publicly accessible web server, removed the data from the web server, and placed it in a secure, quarantined location. DTS was also informed that two instances of confidential data from the Wentworth website also resided in the Google cache. Requests were immediately sent to Google to have the data removed. Google removed both instances within 12 hours of each request, with the final instance being removed the evening of December 24, 2010. DTS began an internal forensic discovery in an effort to determine the history of any unauthorized access. The affected website was set up on April 10, 2007, with browsing access enabled for internal access; thus, the data was also searchable by the public. DTS reviewed Internet Information Server (IIS) logs; however, the logs had been turned off due to the tremendous amount of activity on the server. Because the logs had been turned off, DTS cannot precisely determine when the unauthorized access actually began other than between April 10, 2007, and December 20, 2010. Other search engines (Ask, Yahoo, Bing, AltaVista, and Excite) were checked to determine if confidential data was in the cache and still publicly available. No other data was found. The immediate response to contain data exposure concluded at this time. The incident was not reported to law enforcement. There has been no evidence that the personal information has been used for fraudulent purposes. However, credit monitoring services are being offered to those affected by the unauthorized access. Wentworth has engaged the services of an attorney and a data security consultant to help create the proper response to the incident.

Pro-active Measures to Avoid Future Incidents

Wentworth has taken multiple measures to eliminate further exposures. The Institute has procured a tool to find and quarantine any personal information stored in an unsecure location. The tool, Identity Finder, is being used to search all public facing servers, local drives on faculty and staff utilized desktops and laptops, and internal servers with broad-based permissions. The process to search all locations will continue into February 2011. During the initial search in December 2010, two additional files containing personal information were found on the same compromised web server and quarantined. The data was located in a separate, distinct folder and unrelated to the previously described Wentworth Opening Week data. These files were not searchable (browsing access disabled) via search engines, and there is no evidence the data has been used for fraudulent purposes.

Additional measures being taken to avoid future exposures:

1. The Wentworth Information Security Committee, comprised of staff institute-wide, meets regularly to continually update policies and procedures, and make recommendations to ensure data security. A meeting to discuss lessons-learned from this incident was held on February 1, 2011.
2. Local and network drives will be scanned monthly to monitor employee compliance when storing personal information.

3. Using the Institute's virus-protection software, employees will be automatically warned if personal information is being copied to an unsecure location.
4. DTS has contracted an outside auditor to complete penetration testing to identify security vulnerabilities for rectification.
5. Wentworth is evaluating encryption software for future implementation in laptops and databases containing personal information.
6. Logging of activity on webservers has been activated for future forensic testing as needed.
7. Reinforce the procedure for reviewing all personal information requests to include an individual review with requestor to clarify need and appropriate protection for data.
8. Establish a policy for length of time information is stored on server or in a database, with yearly reviews.

OTHER NOTIFICATION AND CONTACT INFORMATION

If you have any questions or need any additional information please contact me using the following contact information:

[redacted]

Sincerely,

Pete Maddocks
Associate VP for Finance

The following letter was sent to 57 New Hampshire residents whose personal information that was subject to unauthorized access did not include allergies, medications, medical conditions, and disabilities that the individual had provided to Wentworth in connection with his/her registration for Wentworth Opening Week.

Date

Name
Address
City, State ZIP

Dear FirstName,

I am writing to notify you of a possible breach of security of your personal information that may have occurred between April 10, 2007, and December 24, 2010.

On December 22, 2010, Wentworth Institute of Technology was notified that an electronic file was accessible on the Institute's website that contained personal information, including your full name, social security number, and date of birth. The file did not include any bank account or credit card account information.

The file could be accessed on Wentworth's website through the use of search engines and targeted searches, and the file was stored (cached) by web search engine Google at some point after April 10, 2007. Upon learning the file was publicly accessible, Wentworth immediately removed it from the Institute's website and collaborated with Google to have the file removed from their web search engine caches.

To help insure that this information is not used inappropriately, Wentworth will cover the cost of credit monitoring and identity protection for one year. To take advantage of this offer, please see the last page of this letter for additional information and instructions for enrollment.

Consumers may place a security freeze on their credit reports. 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. Please also note, if you plan on signing up for the complimentary service outlined on page 4, we recommend that you don't place a credit freeze until after enrollment because it can delay the receipt of your membership materials.

A credit reporting agency may charge you 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

TransUnion 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 and date of birth;
3. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five (5) years;
4. Proof of current address such as a current utility bill or telephone bill;
5. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
6. 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 (3) 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.

We also advise you to immediately take the following steps:

- Call the toll-free number of any one of the three (3) major credit bureaus (see below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

  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 9532
  Allen, TX 75013

  TransUnion
  1.800.680.7289
  www.transunion.com
  Fraud Victim Assistance Department
  P.O. Box 6790
  Fullerton, CA 92834-6790

- Order your credit reports. By establishing a fraud alert, as outlined above, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an account has not been opened with your personal information.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. Wentworth Institute of Technology apologizes for the stress, worry and inconvenience this situation has caused you and is doing everything it can to rectify the situation.

If you have any further questions or concerns, please contact Wentworth by email at infosecurity@wit.edu, or by telephone at 800.222.9368, choose option 8 at the voice prompt.

Sincerely,

Pete Maddocks
Associate VP for Finance
Wentworth Institute of Technology
550 Huntington Avenue
Boston, MA 02115

Free Credit Monitoring and Identity Theft Protection

Complimentary Service Offer

Wentworth would like to offer you a free one-year subscription to ITAC Sentinel® Plus, a credit monitoring and identity theft protection service. ITAC Sentinel Plus provides essential monitoring and protection of not only credit data, but also monitors the Internet for personal data such as social security number, bank accounts, and credit card accounts on websites known to be frequented by identity thieves. This program is provided by Intersections Inc. (NASDAQ: INTX), a leading provider of consumer and corporate identity risk management services.

ITAC Sentinel® Plus features include:

- 3-bureau credit report and scores
- 3-bureau daily monitoring with NOTIFY EXPRESS® alerts
- 3-bureau quarterly credit update
- ITAC victim assistance
- Card theft protection
- Internet surveillance
- Credit education specialists
- Up to $20,000 identity theft insurance with $0 deductible.*

If you wish to take advantage of this comprehensive monitoring service, you must enroll by April 12, 2011.

Enrollment Procedure

To activate this coverage, please call the toll-free number or visit the website listed below and enter the redemption code. The redemption code is required for enrollment, and can only be used one time by the individual addressed.

Toll-Free:	1.866.758.4463
	(this toll-free number will be activated by January 20, 2011)
Web Site:	www.itacsentinel.com/alert
Redemption Code:	

In order to enroll, you will need to provide the following personal information:

- Mailing address
- Phone number
- Social security number
- E-mail address
- Redemption code

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We apologize for any inconvenience and urge you to enroll today.

*Insurance underwritten by Travelers Casualty and Surety Company of America and its property casualty affiliates, Hartford, CT 06183. Coverage for all claims or losses depends on actual policy provisions. Availability of coverage can depend on underwriting qualifications and state regulations.

The following letter was sent to 31 New Hampshire residents whose personal information that was subject to unauthorized access did include allergies, medications, medical conditions, and disabilities that the individual had provided to Wentworth in connection with his/her registration for Wentworth Opening Week.

Date

Name
Address
City, State ZIP

Dear FirstName,

I am writing to notify you of a possible breach of security of your personal information that may have occurred between April 10, 2007, and December 24, 2010.

On December 22, 2010, Wentworth Institute of Technology was notified that an electronic file was accessible on the Institute's website that contained personal information, including your full name, social security number, and date of birth. The file also included any information such as allergies, medications, medical conditions, and disabilities that you provided to Wentworth in connection with registration for Wentworth Opening Week. The file did not include any bank account or credit card account information.

The file could be accessed on Wentworth's website through the use of search engines and targeted searches, and the file was stored (cached) by web search engine Google at some point after April 10, 2007. Upon learning the file was publicly accessible, Wentworth immediately removed it from the Institute's website and collaborated with Google to have the file removed from their web search engine caches.

To help insure that this information is not used inappropriately, Wentworth will cover the cost of credit monitoring and identity protection for one year. To take advantage of this offer, please see the last page of this letter for additional information and instructions for enrollment.

Consumers may place a security freeze on their credit reports. 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. Please also note, if you plan on signing up for the complimentary service outlined on page 4, we recommend that you don't place a credit freeze until after enrollment because it can delay the receipt of your membership materials.

A credit reporting agency may charge you 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

TransUnion 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 and date of birth;
3. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five (5) years;
4. Proof of current address such as a current utility bill or telephone bill;
5. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
6. 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 (3) 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.

We also advise you to immediately take the following steps:

- Call the toll-free number of any one of the three (3) major credit bureaus (see below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

  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 9532
  Allen, TX 75013

  TransUnion
  1.800.680.7289
  www.transunion.com
  Fraud Victim Assistance Department
  P.O. Box 6790
  Fullerton, CA 92834-6790

- Order your credit reports. By establishing a fraud alert, as outlined above, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an account has not been opened with your personal information.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. Wentworth Institute of Technology apologizes for the stress, worry and inconvenience this situation has caused you and is doing everything it can to rectify the situation.

If you have any further questions or concerns, please contact Wentworth by email at infosecurity@wit.edu, or by telephone at 800.222.9368, choose option 8 at the voice prompt.

Sincerely,

Pete Maddocks
Associate VP for Finance
Wentworth Institute of Technology
550 Huntington Avenue
Boston, MA 02115

Free Credit Monitoring and Identity Theft Protection

Complimentary Service Offer

Wentworth would like to offer you a free one-year subscription to ITAC Sentinel® Plus, a credit monitoring and identity theft protection service. ITAC Sentinel Plus provides essential monitoring and protection of not only credit data, but also monitors the Internet for personal data such as social security number, bank accounts, and credit card accounts on websites known to be frequented by identity thieves. This program is provided by Intersections Inc. (NASDAQ: INTX), a leading provider of consumer and corporate identity risk management services.

ITAC Sentinel® Plus features include:

- 3-bureau credit report and scores
- 3-bureau daily monitoring with NOTIFY EXPRESS® alerts
- 3-bureau quarterly credit update
- ITAC victim assistance
- Card theft protection
- Internet surveillance
- Credit education specialists
- Up to $20,000 identity theft insurance with $0 deductible.*

If you wish to take advantage of this comprehensive monitoring service, you must enroll by April 12, 2011.

Enrollment Procedure

To activate this coverage, please call the toll-free number or visit the website listed below and enter the redemption code. The redemption code is required for enrollment, and can only be used one time by the individual addressed.

Toll-Free:	1.866.758.4463 (this toll-free number will be activated by January 20, 2011)
Web Site:	www.itacsentinel.com/alert
Redemption Code:	

In order to enroll, you will need to provide the following personal information:

- Mailing address
- Phone number
- Social security number
- E-mail address
- Redemption code

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We apologize for any inconvenience and urge you to enroll today.

*Insurance underwritten by Travelers Casualty and Surety Company of America and its property casualty affiliates, Hartford, CT 06183. Coverage for all claims or losses depends on actual policy provisions. Availability of coverage can depend on underwriting qualifications and state regulations.