COLLEGE OF THE HOLY CROSS

Timothy F. Mines
General Counsel

October 7, 2011

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

Re: College of the Holy Cross Data Security Event

Dear Attorney General Delaney:

Pursuant to New Hampshire Rev. Stat § 359-C:20, we are writing to notify you of a data security event that compromised the security of various employee e-mail accounts at The College of the Holy Cross ("Holy Cross"). We are informing your office of facts related to this event which are known at this time, and of the actions being taken in response. Holy Cross has retained computer forensic experts, Cybertrust, and breach notification legal counsel, Nelson, Levine, de Luca & Horst, LLC, to assist with its investigation of and response to this incident. The investigation is ongoing and should new facts be learned we will supplement this notice to you.

Nature of the Security Event

On Friday, September 9, 2011, a Human Resources ("HR") staff member received a phishing email that fraudulently appeared to be from the "System Administrator." The email requested that the HR staffer provide her user name and password for her email account, which she did. On Saturday, September 10, 2011, her entire email account was erased. Holy Cross's IT Security Department was notified of the missing email accounts on September 12, 2011, at which time they began investigating the intrusion. It was discovered that six (6) additional staff members had similarly been defrauded into providing their account information and had their email accounts erased.

Number of New Hampshire Residents Affected

Holy Cross' IT restored all lost emails from its back-up sources. There were over 30,000 email messages from the seven (7) staff member email accounts that were lost or stolen. A review of these email messages and all attachments thereto revealed that personal information, consisting of name plus social security number, and/or driver's license number, and/or financial account information, of four New Hampshire residents may have been compromised. All such

personal information was found within emails contained only on the HR staffer's email account. None of the other six (6) email accounts contained personal information. The affected residents will be receiving written notification of the breach via first class mail in compliance with New Hampshire Rev. Stat § 359-C:20(a). This notification will be substantially in the form of the sample letter attached hereto and will be mailed on October 6, 2011.

It is the policy of Holy Cross that sensitive personal information, such as social security numbers and financial account numbers, must not be shared via email unless the information is encrypted. This policy is part of Holy Cross's written information security plan, which is attached hereto for your review. Unfortunately, there were email messages in the HR staffer's account that contained unencrypted personal information, which is the reason the affected individuals are being notified. Holy Cross has taken the following steps in response to this breach of its policies:

- Required immediate retraining on the Written Information Security Plan for all staff members whose email accounts were improperly accessed.
- Created a new webpage for cyber awareness on Holy Cross webpage at http://offices.holycross.edu/helpdesk/safe.
- Notified the entire Holy Cross Community by email of additional "phishing" attacks.
- Placed posters throughout the campus regarding "phishing" attacks and security of personal information. See http://offices.holycross.edu/helpdesk/safe/posters.
- Created a procedure to ensure all HR employees re-read the following Policies and procedures: WISP, HR Data handling procedures, Data Retention policies, Data Classification polcies, and Data Destruction policies.
- Conducted 1-hour lecture presented to Human Resources Department on Massachusetts Data Security Law and encryption.
- Purchased SANS "Securing the Human" mandatory online training for the entire College which should be available for presentation within the next two weeks.

Other Steps Taken and to be Taken

On September 15, 2011 all Holy Cross faculty and staff were informed via email correspondence from General Counsel and the Data Security Manager about the phishing attacks. They were reminded what phishing attacks were and of how they can protect Holy Cross from further attempts at unauthorized access to email accounts. On October 10, 2011 all staff department heads will be provided with additional information regarding the phishing attacks.

Holy Cross retained privacy counsel to assist it as it develops its response. Privacy counsel contacted the FBI and will also be contacting the FTC to determine whether these

agencies can be of any assistance in preventing further attacks by the perpetrators. Holy Cross's Public Safety Chief will be filing a report with the local police department in Worcester.

Holy Cross's IT staff determined that the phishing attacks originated in Nigeria and Ghana. The FBI confirmed that Nigeria has been the source of similar attacks for years. Holy Cross's IT department is currently blocking all electronic communications from the continent of Africa as a temporary measure while the forensic investigation is conducted and further procedures are implemented to mitigate similar attacks.

A total of 493 individuals from 20 other jurisdictions whose personal information may have been compromised are also being notified of this data security event in accordance with the laws of those jurisdictions. Although we received no evidence that any affected individuals' personal information has been misused, all individuals receiving notification, including those in New Hampshire, are being offered one year of credit monitoring services, as well as identity fraud insurance and identity restoration assistance.

Other Notification and Contact Information

Should you have any questions regarding this notification or other aspects of the data security event please contact our data privacy counsel, John F. Mullen of the law firm Nelson, Levine, de Luca & Horst, at

Sincerely,

Timothy F. Mines

Timothy F. Mines, Esq.
General Counsel

Encl.

Holy Cross

C/O ID Experts
PO Box 6336
Portland, OR 97228-6336

[Date]

[Name]
[Address]
[City/State/Zip]

[Dear Name:]

I am writing today with important information that affects you.

The College of the Holy Cross discovered on September 12, 2011 that some of its private information was unlawfully accessed. Our ongoing investigation indicates that **your personal information, including your name and your Social Security number and date of birth, may have been accessed or taken.** We have specific information regarding what data of yours is involved and will provide guidance to assist you in addressing potential consequences from the exposure of your personal information. We recommend that you **contact our hotline at 1-888-288-9625**, Monday through Friday from 9 am - 9 pm Eastern.

I want to assure you that Holy Cross takes this matter very seriously. Your safety and security as a member of this community is our highest priority. The College has retained computer forensic experts and has retained legal experts to assist with our ongoing investigation. We are taking a series of steps to ensure that this does not happen again.

We have retained the firm of ID Experts® to assist you with any questions related to this security incident. I encourage you to be in touch with these experts. As always, our staff in the Human Resources department is available to assist you if you have any questions or need more information. Your questions specific to this security incident, however, are best answered by the experts.

ID Experts® will provide you with FraudStop™ credit monitoring and identity recovery services to help protect your identity, should you determine that such services are appropriate. With this protection—which is free of charge to you—ID Experts will help you resolve issues if your identity is compromised. We encourage you to register for this free identity protection service by calling 1-888-288-9625. Please note the deadline to enroll is April 3, 2012.

Your free one-year membership will include the following:

- **Fraud Resolution Representatives:** ID Experts will provide assistance if you suspect that your personal information is being misused. A recovery advocate will be assigned to your case, and they will work with you to assess, stop, and reverse any fraudulent activity. If you suspect or

discover suspicious activity, you should contact them immediately for assistance.

- **Credit Monitoring:** ID Experts will provide 12 months of credit monitoring that will notify you by email of key changes in your credit file. Detailed instructions for activating your credit monitoring are provided on the ID Experts member website which you may log into once you enroll.

- **Exclusive Educational Materials:** The ID Experts website includes a wealth of useful information, including instructive articles, a Protection Test that you can take, very helpful ID Self-Defense Academy™ and a place where you can review and update your account. Their experts will keep you up-to-date on new identity theft scams, tips for protection, legislative updates and other topics associated with maintaining the health of your identity.

- **Insurance Reimbursement:** ID Experts will arrange $20,000 of identity theft reimbursements for certain expenses that can be incurred when resolving an identity theft situation.

Representatives from ID Experts can answer questions or concerns you may have regarding this incident and the protection of your personal information. They are available Monday through Friday from 9 am - 9 pm Eastern Time by calling 1-888-288-9625.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. You will need to reference the following membership code. Please have this letter with you when calling.

Your Membership Code: [ID Experts will insert individual codes]

To protect against possible identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

The names and contact information of the three major U.S. credit bureaus are listed below. At no charge, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

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

To further educate yourself regarding identity theft and the steps you can take to avoid identity theft, you may contact the Federal Trade Commission. They can be reached at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/bcp/edu/microsites/idtheft/
1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; telephone (919) 716-6400; or www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; telephone: (888) 743-0023; or www.oag.state.md.us.

Again, please be assured that your safety and security is very important to us. We regret any inconvenience or concern that this matter may have caused you. If you have any questions, please contact the experts at the call center dedicated to this matter Monday through Friday from 9 am - 9 pm Eastern Time by calling 1-888-288-9625.

Very truly yours,

Michael C. McFarland, S.J.
President
College of the Holy Cross