University of Delaware IT security breach FAQ–UPDATED 8.2.13 & REVISED 8.2.13
To be linked by section prominently from www.udel.edu/it/security.

We remind you to safeguard your private information. The University will not contact those affected to ask you to confirm any of your personal information. If an unknown person should contact you and claim that he or she can help you, please do not surrender any personal information. No one from the University, Kroll Advisory Solutions or any other reputable organization will contact you to request your confidential material.

PART I: ABOUT THE CYBERATTACK

What happened?
On July 22, 2013, the University of Delaware discovered a cyber security breach during routine systems maintenance.

The University of Delaware is notifying the campus community that files were taken that include confidential personal information of current and past employees, including student employees. A criminal attack on one of the University's systems took advantage of a vulnerability in software acquired from a vendor.

The University sent notification letters dated July 29, 2013, to more than 72,000 affected persons and offered them free credit monitoring. Approximately one-third have active UD email accounts and will have received an email notification as well.

Who is affected?
While we are still working to determine the scope of the breach, we do know that information about current and past employees—including student employees—was exposed.

What information did the files contain?
Information in the compromised files includes names, addresses of record, Social Security numbers and UD IDs (employee identification numbers).

When did this happen?
The cyberattack occurred on or about July 17, 2013.

How did this happen?
UD has engaged a leading data security firm to determine what happened and where the breach may have come from; what other University maintained systems, if any, may have been attacked; and whether other confidential information, if any, may have been exposed. UD has also reported this incident to FBI officials.

Several dozen other companies, agencies, and organizations have also been subjected to attacks taking advantage of the same software vulnerability.

Who is responsible for this breach?
We don't know at this point, but we are working with both the FBI and a leading data security firm to determine what happened and where the breach may have come from; what other UD-

maintained systems, if any, may have been attacked; and whether any other confidential information may have been exposed.

The University of Delaware takes the security of information very seriously. Even though the forensic investigation is not complete, we are taking steps to strengthen our defenses against future cyberattacks.

Who is going to cover costs involved?
The University's priority is to protect those who may be at risk due to this cyberattack by providing credit monitoring services. UD will be providing these services at no cost to you.

Additionally, UD is employing a leading data security firm to complete a forensic investigation of the incident to ensure a thorough evaluation of how this breach happened and the most secure path going forward to protect against future attacks.

The costs UD is incurring for the investigation and services for those affected will not be passed along to any UD constituency.

Is this a trend in higher education?
According to an article that appeared on July 16, 2013, in *The New York Times,* many large research universities across the country have been subjected to attacks over the last days and weeks. Like most of the other universities subject to these cyber incidents, UD has been working within the parameters of industry best practices to secure our systems.

The incident at the University of Delaware is neither unique nor the largest security breach in higher education. The University is doing everything it can to help you monitor the risk to your personal information.

PART II: FOR THOSE AFFECTED

Is my UD email account affected by this incident?
At this time, there is no evidence that UD email accounts or UD email has been affected by this security breach .

What should I do?
The University sent notification letters to all who were affected. If you are currently or were a full-time, part-time or student employee of the University of Delaware, you may be included in this group. These notifications provide specific instructions on what affected individuals may choose to do as well as information on additional resources.

If your information is at risk, the most important thing you can do is to monitor your credit information. To help relieve concerns and restore confidence following this incident, the University has contracted with Kroll Advisory Solutions to assist you—at no cost to you.

What can the University and Kroll Advisory Solutions do for those whose information is at risk?
If you are affected, Kroll Advisory Solutions is providing **identity theft safeguards at no cost to you for a three-year period through its ID TheftSmart™ program**. Kroll Advisory Solutions is a global leader in risk mitigation and response services to universities and other clients affected by large-scale cyberattacks.

Do I have to pay for Kroll's services?
UD is providing those affected with access to Kroll Advisory Solutions–at no cost.

What services will Kroll offer me?
The two most important services UD is offering through Kroll are credit monitoring and identity theft consultation services.

First, UD is providing free access to Kroll's credit monitoring service for 36 months. You must activate within six months from the date of the notification. Once activated, you will be notified by email when your credit files show certain credit activity in your name that is commonly associated with identify theft.

Second, UD is providing free access to Kroll's licensed investigators for three years from the date of notification. Kroll's team has expertise in solving problems associated with identity theft and potential identity theft. The investigators will be available to listen to your concerns, answer your questions and offer their expertise regarding any issues you may have noticed. Should your credit be affected by this incident, an investigator will help you restore your identity to pre-theft status. This service will be provided at no cost to you.

How do I get started with Kroll?
Follow the instructions on how to enroll in Kroll's credit monitoring service contained in the notification letters sent to those affected.

In the notification letter, each affected individual was given a unique membership number that you will need to provide when you sign up for Kroll's services. You can sign up online at www.idintegrity.com or by filling out and returning the *Consumer Credit Report and Credit Monitoring Authorization Form* that was enclosed with your notification letter.

What should I do if I have questions about Kroll's program or problems signing up?
Contact Kroll directly at 1-877-309-0016. When you call, you will be asked to provide your unique membership number, which was listed in the letter/email. If you have not yet received a notification, you can still call Kroll.

I am an affected individual but I have not received email yet, should I be concerned?
Some email messages from Kroll Advisory Solutions are being diverted into recipients' spam, junk or trash folders. If you have not received an email, please check there.

We do not have email addresses for all affected persons. However, letters have been sent via U.S. Mail to all those affected.

Can I enroll for credit monitoring services with Kroll Advisory Solutions if I was not affected by this incident?
The services being provided by Kroll Advisory Solutions are available only to those who are affected by this security breach. However, there is information available on our IT Security Response website about identity theft and steps you can take to protect your identity.

I think something already happened to my credit information. How do I contact an investigator?
Even if you choose not to activate the credit monitoring service, Kroll's licensed Investigators are standing by to answer questions or help you with any concerns you may have. Call 1-877-309-0016.

Are there any additional precautions I should take?
There are additional steps you can take to protect yourself against the consequences of identity theft.

- Place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Call any one of the three credit reporting agencies and (1) request that a fraud alert be placed on your account and (2) order a free credit report from the agency. The agency can also provide you with information on placing a "security freeze" on your account.
    - **Equifax Information Services, LLC:** 1-888-766-0008
    - **Experian:** 1-888-397-3742
    - **TransUnion LLC:** 1-800-680-7289
- Carefully review your credit reports for accounts you did not open or for inquiries from creditors that you did not initiate. Review your personal information, such as home address and Social Security number for accuracy. If you see anything you do not understand, call the credit agency at the telephone number on the report.

What's the difference between the monitoring services Kroll offers and those that Equifax, TransUnion, and Experian are offering?
Kroll Advisory Solutions is providing identity theft safeguards at no cost to you for a three-year period through its ID TheftSmart™ program. Once activated, you will receive email alerts

whenever there are certain changes in your credit file—opening a new account, issuing a new card, changes of address, for example. This service will be provided at no cost to you. For more information, see Kroll's ID TheftSmart™ brochure or log on to the www.idintegrity.com website, select **Learn More**, then select **About Credit Monitoring.**

Equifax, TransUnion, and Experian offer other services, some of which are free and some of which require a payment. (The information below is adapted from the Equifax website.)

A Fraud Alert (free for 90 days) is a notice added to your credit file that you may be a victim of fraud and requires creditors using the file to contact you to verify your identity prior to establishing any new credit accounts in your name, issuing a new card on an existing account, or increasing the credit limit on an existing account.

A Security Freeze (requires fees) prevents your credit report from being reported to third parties, except those exempted by law or those for whom you contacted a credit reporting service and requested that the freeze be lifted.

For more information consult the Equifax, TransUnion, and Experian websites.

Am I a victim of identity theft?
Although we have no evidence that any unauthorized individual or entity has actually used any of your personal information, we are bringing this data breach to your attention so you can be aware of the risk. You should be alert to signs of any possible misuse of your personal information now and in the immediate future.

Should I notify the authorities if I see suspicious activity on my credit report?
If you find any suspicious activity on your credit reports, call local law enforcement authorities and the state attorney general's office.

If you think you are the victim of identity theft, notify the United States Federal Trade Commission: 1-877-ID-THEFT (1-877-438-4338).

Should I be concerned about my UD PIN or UDelNet ID and password?

Because of this incident, all PINs associated with UD IDs were reset. As of 5 p.m., Aug. 1, 2013, self-service PIN reset is now enabled for Blue Hen incoming students, current undergraduate students and current graduate students. Details are available at http://www.udel.edu/it/help/CAS/udid.html.

Alumni who need to reset their PINs should call the Registrar's Office at 302-831-2132. Due to the volume of PIN resets taking place, only those students enrolling for courses and alumni who need immediate access to their academic record can be accommodated at this time.

Employees who use PINs may reset their own PINs or see their HR liaison if they do not know their UDelNet ID and password.

A reminder has been added to the Central Authentication Service (CAS) page that PIN reset is required if you use UD ID and PIN. This reminder notes that any PIN set before July 30, 2013, must be reset and directs users to click on the "Forgot your UD ID or Pin?" link on the page to reset it.

For more information, see the IT PIN reset page available from any CAS page or at http://www.udel.edu/it/help/CAS/udid.html.

UDelNet IDs and passwords were not affected. Students or employees who use a UDelNet ID and password to log on and who do not use their PIN will not need to reset it.

Should I be concerned about my retirement accounts?

Information related to retirement accounts is not included in the data that was taken.

Is my family's information at risk?
Information about family members is not included in the data that was taken; however, if a member of your family was ever employed by UD, it is possible that his or her information may have been affected by this incident. Affected individuals will be notified directly.

I am a donor to UD. Is my personal information at risk from this incident?
This security breach did not affect any University Development and Alumni Relations databases and no information there was compromised. However, anyone who is or has been an employee of the University, including student employees, may be affected.

PART III: SECURITY MEASURES

Where can I get information on updates?
UD will post updates to this website.

What steps did the University take once it found out about the attack?
UD took immediate corrective action to contain the incident. Although we cannot discuss the technical details of our systems and network security, we can tell you that the University is working with the FBI and has engaged a leading data security firm to assist with the forensic investigation.

What is being done to ensure this does not happen again?
The University of Delaware treats information security with the utmost seriousness and continually updates its defenses against cyberattacks.

The University has been aligned with the best practices in the IT industry; unfortunately, there is no way that any organization can guarantee that a cyberattack will never occur. However, we

are already making changes to our network in consultation with the FBI, our data security consultant and other universities whose systems have been breached in the past.

How will UD manage my private information in the future?
Our information security policies and practices are in line with both IT industry and higher education IT best practices. UD follows HIPAA, FERPA and all other federal and state laws designed to protect your private information. UD will continue to exercise caution and continually improve safeguards for sharing your personal information.

Why does UD need to have my Social Security number at all?

The Higher Education Act of 1965 allows colleges and universities to use Social Security numbers (SSNs) for institutional transactions. It is routine for colleges and universities to store this information electronically. According to the U.S. Social Security Administration, it is a best practice in higher education for an institution to assign another primary identifier for most university transactions while the SSN remains in the university database as a secondary identifier. That is what we do at UD. For employees, a "University of Delaware Identification Number" (UD ID) is assigned when an employee is hired and appears on most university forms as that employee's identifier. The same process of assigning unique UD ID identification numbers is used for students. Your UD ID cannot be used by itself to access your private information. SSNs do not appear on UD-issued identification cards, procurement cards, or any UD public posting.

UD collects and uses SSNs only as necessary for the performance of the University's duties and responsibilities and as required by law. The University uses the SSN as a unique identifier for many business and financial purposes:(1) to process payroll and other human resource information, including health and retirement benefits registration and processing, tax reporting, unemployment and workers compensation, (2) for payments to vendors and independent contractors, (3) as part of the process of making financial aid awards, including grants, loans, work-study awards, and other forms of financial aid, (4) for student account collections, (5) as part of admissions and enrollment processes, and (6) to facilitate planned giving reporting.

UD is dedicated to ensuring the privacy and proper handling of SSNs of its students, employees, and individuals associated with the University.

Will the University change the way they store Social Security numbers as a result of this incident?
We continually assess and improve our information security policies and procedures to ensure we are in line with both IT industry and higher education IT best practices. Further, we are evaluating our systems and processes in consultation with the FBI, our data security consultant and other universities whose systems have been breached in the recent past. UD complies with HIPAA, FERPA and all other federal and state laws designed to protect your private information. UD will continue to exercise caution and continually improve safeguards for protecting your personal information.