



Norton Rose Fulbright US LLP  
Tabor Center  
1200 17th Street, Suite 1000  
Denver, Colorado 80202-5835  
United States

Direct line +1 303 801 2732  
david.navetta@nortonrosefulbright.com

Tel +1 303 801 2700  
Fax +1 303 801 2777  
nortonrosefulbright.com

June 3, 2016

**Via Federal Express**

Office of the Maryland Attorney General  
**Attn: Security Breach Notification**  
200 St. Paul Place  
Baltimore, MD 21202

**Re: Legal Notice of Information Security Incident**

Dear Sirs or Madams:

I write on behalf of my client, Marymount University ("Marymount") to inform you of a security incident involving personal information provided to Marymount that affected approximately nine Maryland residents. Marymount is notifying these individuals and outlining some steps they may take to help protect themselves.

On May 13, 2016, Marymount learned that an unauthorized individual may have gained access to some of its systems during two brief overnight periods on May 13 to May 14, 2016 and May 15 to May 16, 2016. Upon learning of this incident Marymount immediately commenced an investigation and reset accessed accounts. Once the investigation determined that the individual was able to use the password reset function on Marymount's intranet site to gain unauthorized access, Marymount promptly disabled access to this function on the morning of May 16, 2016. Marymount believes that the incident may have affected certain personal information, including name, Social Security number, and, for some employees, bank account information.

Marymount takes the privacy of personal information seriously, and deeply regrets that this incident occurred. Marymount took immediate steps to address and contain this incident upon discovery, including resetting accounts that had been accessed and, as outlined above, disabling the password reset function to prevent additional accounts from being accessed in this manner. Marymount is also currently working to enhance the password reset function to help prevent recurrences of unauthorized access and will not re-enable this function until those enhancements are complete. While Marymount is continuing to review its systems and enhance security measures, it believes the incident has now been contained. Marymount has also contacted local and federal law enforcement and will continue to cooperate with their investigation of this incident.

Affected individuals are being notified of the incident via a written letter, which includes an offer of 24 months complimentary identity protection and fraud resolution services. The notifications will begin mailing on or about June 3, 2016. A form copy of the notice being sent to the affected Maryland residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or [kris.kleiner@nortonrosefulbright.com](mailto:kris.kleiner@nortonrosefulbright.com).

Very truly yours,

A handwritten signature in black ink, appearing to read 'Kristopher Kleiner', with a long horizontal flourish extending to the right.

Kristopher Kleiner

KCK  
Enclosure



June 3, 2016

<First Name> <Last Name>

<Address Line 1>

<Address Line 2>

<City>, <State> <Zip>

Dear <First Name>,

### **Notice of Security Incident**

We recently learned that Marymount University was the victim of a security incident that may have affected some of our employees' personal information. We are providing this notice as a precaution to formally inform potentially affected employees about the incident and to call your attention to some steps you can take to help protect yourselves. Some of this information may have already been shared with you in previous communications about this incident. We apologize for any frustration or concern this may cause you. We have arranged for you to receive identity protection services for one year at no cost to you. Instructions for enrolling in these services can be found in the "Information about Identity Theft Protection" page attached to this letter.

#### ***What Happened***

We recently learned that an unauthorized individual may have gained access to some of our systems during two brief overnight periods on May 13 to May 14, 2016 and May 15 to May 16, 2016. We immediately commenced an investigation, and reset accessed accounts. Once our investigation determined that the individual was able to use the password reset function on our intranet site to gain unauthorized access to our systems, we promptly disabled access to this function on the morning of May 16, 2016.

#### ***What Information Was Involved***

We believe that the incident may have affected certain employees' personal information available on our intranet, including name, address, phone number, email address, Social Security number, wage information, and, for some employees, bank account information and the name and Social Security number of their spouse and dependents.

#### ***What We Are Doing***

The security of your personal information is of utmost importance to us. Accordingly, we took immediate steps to address and contain this incident upon discovery, including resetting accounts that had been accessed and, as outlined above, disabling the password reset function to prevent additional accounts from being accessed in this manner. We are also currently working to enhance the password reset function to help prevent recurrences of unauthorized access and will not re-enable this function until those enhancements are complete. While we are continuing to review our systems and enhance our security measures, we believe the

2807 North Glebe Road | Arlington, Virginia 22207-4299

[www.marymount.edu](http://www.marymount.edu)



incident has now been contained. We have also contacted federal law enforcement and we will continue to cooperate with their investigation of this incident.

### ***What You Can Do***

We want to make you aware of steps you can take to guard against possible fraud or identity theft.

First, to help protect your identity, we are offering ***two years of complimentary identity protection services*** from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the ["Information about Identity Theft Protection"](#) page attached to this letter.

Please also ***review the remaining sections in the "Information about Identity Theft Protection" page***, as they describe additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

We recommend that you ***carefully check your credit reports*** for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. We also recommend that you ***review credit and debit card account statements*** as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should immediately notify the issuer of the credit or debit card.

### ***For More Information***

Please contact me for more information about this incident, or if you have additional questions or concerns. My contact information is included below. Again, we sincerely regret that this incident has occurred and any inconvenience or concern caused by this incident.

Sincerely,

Steve Munson

Executive Director, IT Services  
Marymount University  
(703) 526-6901  
[smunson@marymount.edu](mailto:smunson@marymount.edu)

2807 North Glebe Road | Arlington, Virginia 22207-4299

[www.marymount.edu](http://www.marymount.edu)