McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

February 17, 2022

VIA EMAIL

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

Re: Point Park University – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Point Park University ("Point Park"). I am writing to provide notification of an incident at Point Park that may affect the security of personal information of approximately two (2) Maryland residents. Point Park's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Point Park does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On January 20, 2022, Point Park received a FedEx package from its payroll company containing employees' year end W2's. Upon inspecting the FedEx package, Point Park noticed that most of the W2's were bundled together with rubber bands, but some were loose in the package. Point Park immediately inspected the individual W2's to determine if they were all there or if some were missing. At the conclusion of this inspection Point Park determined that some employees' W2's were not in the FedEx package. Point Park immediately contacted the payroll company to confirm that they had printed and sent all of the W2's. Point Park also contacted FedEx to investigate the incident and to see if they could locate the missing W2's. The payroll company recently confirmed that all employee W2's were printed and included in the FedEx package. FedEx is still investigating and trying to locate the missing W2's.

During the course of this investigation, some recipients of the missing W2's have received them via the US Postal Service. However, Point Park has not received confirmation that all of the W2's that were missing from the FedEx box actually made it to the intended recipients via US Mail. Upon learning of this issue, Point Park immediately commenced a prompt and thorough investigation. As part of their investigation, Point Park has been working very closely with external cybersecurity professionals experienced in handing these types of incidents.

At the time of this notification, Point Park is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Point Park wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Point Park is providing the affected residents with written notification of this incident commencing on or about February 17, 2022 in substantially the same form as the letter attached hereto. Point Park is offering the affected residents complimentary one-year membership with a credit monitoring service. Point Park will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Point Park will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Maryland Attorney General, and the Federal Trade Commission.

At Point Park, protecting the privacy of personal information is a top priority. Point Park is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Point Park continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

James J. Giszczak

Encl.

POINT PARK UNIVERSITY

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

RE: CREDIT MONITORING

[redacted]

[redacted]

[redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Point Park University. We're writing with important information regarding a recent data security incident that may have involved some of your information. We want to provide you with information about the incident, let you know about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

IMPORTANT NOTE: If you have received your 2021 ORIGINAL Form W-2 in a sealed blue envelope, you can ignore this letter.

What Happened?

On January 20, 2022, Point Park University received a Fed Ex package from its payroll company containing employees' year end W2's. Upon inspecting the Fed Ex package, we noticed that most of the W2's were bundled together with rubber bands, but some were loose in the package. We immediately inspected the individual W2's to determine if they were all there or if some were missing. At the conclusion of this inspection we determined that some employees' W2's were not in the Fed Ex package. We immediately contacted the payroll company to confirm that they had printed and sent all of the W2's. We also contacted Fed Ex to investigate the incident and to see if they could locate the missing W2's. The payroll company recently confirmed that all employee W2's were printed and included in the Fed Ex package. Fed Ex is still investigating and trying to locate the missing W2's.

During the course of this investigation, some recipients of the missing W2's have received them via the US Postal Service. However, we have not received confirmation that all of the W2's that were missing from the Fed Ex box actually made it to the intended recipients via US Mail.

What We Are Doing.

Upon learning of this issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handing these types of incidents. Although there is a possibility that Fed Ex finds the missing W2's, or that you will receive your W2 via US Mail, we wanted to notify you of this incident.

<u>What Information Was Involved.</u>

The W2's contained some of your personal information, including your name and Social Security number.

<u>What You Can Do.</u>

To protect you and your information, we are providing you with 12 months of free credit monitoring and identity theft protection services through TransUnion. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This service is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

If your tax return is rejected **<u>or</u>** you receive a tax notice from a government agency (such as a notice from the IRS indicating someone was otherwise using your Social Security number), we recommend that you follow the below guidance:

-
- Respond immediately to any IRS notice you receive, and call the number provided and/or follow the instructions contained in the notice;
- **File an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf).** ;
    - ***Additional instructions for filing the Affidavit are included on the following pages***.
- You may choose to opt-in to the IRS Identity Protection (IP) PIN Program. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. To opt-in, you should use the online "Get an IP PIN" tool (which can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin). If you don't already have an account on IRS.gov, you must register to validate your identity. An IP PIN is valid for one calendar year. You must obtain a new IP PIN each year. The IP PIN tool is generally unavailable mid-November through mid-January each year.
- If you are filing Form 14039, you should also check with your local state tax agency to see if there are any additional steps to take at the state level for reporting tax-related identity theft;
    - A complete listing of each state tax agency's website can be found at: https://www.taxadmin.org/state-tax-agencies. ***Additional information for reporting tax-related identity fraud to state tax agencies can be found on the following pages.***
- Review guidance from the IRS about tax-related identity theft at: https://www.irs.gov/uac/taxpayer-guide-to-identity-theft (*Taxpayer Guide to Identity Theft*) and https://www.irs.gov/pub/irs-pdf/p5027.pdf (*IRS Publication 5027, Identity Theft Information for Taxpayers*); and/or
- Call or visit your local law enforcement agency and file a police report.

Keep in mind that if you have an open identity theft case that is being worked on by the IRS, you need to continue to file your tax returns while the investigation is ongoing. Additional information regarding preventing tax related identity theft can be found at: http://www.irs.gov/uac/Identity-Protection.

For More Information.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. The response line is available Monday through Friday, 9am to 9pm Eastern, excluding all major U.S. holidays.

Sincerely,

Point Park University

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the myTrueIdentity website at [redacted] and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at [redacted]. When prompted, enter the following 6-digit telephone pass code [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and [redacted] Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more.

The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: [redacted], Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	***Experian***	***TransUnion LLC***
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, PA 92834-6790
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	https://www.experian.com/fraud/center.html	https://www.transunion.com/fraud-alerts
(800) 525-6285	(888) 397-3742	(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (800) 349-9960	***Experian Security Freeze*** P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742	***TransUnion Security Freeze*** P.O. Box 2000 Chester, PA 19016 http://www.transunion.com/credit-freeze (888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been misused, you may file a police report in the city in which you currently reside.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland**,** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.