

October 30, 2024

VIA Electronic Mail: Idtheft@oag.state.md.us

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of a Data Security Incident

To The Office of the Attorney General:

I write on behalf of Perdoceo Education Corporation (“PEC”), as custodian of records for Briarcliffe College (the “School”). Financial Business and Consumer Solutions, Inc. (“FBCS”), a vendor performing debt collection services on the School’s behalf, was recently the target of a cybersecurity incident, in which personal information of former students of the School was involved.

I. Nature of the Security Incident

On February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. This incident did not impact computer systems outside of FBCS’s network, including any systems belonging to the School. FBCS’ investigation determined that the environment was subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access, including information held on behalf of the School.

Following initial notice of the incident, FBCS informed PEC that its investigation and review of the data remained ongoing. As the investigation continued, FBCS informed PEC that personal information relating to students at the School may have been involved in the incident. FBCS had previously informed PEC that it would be handling notifications on behalf of PEC in relation to such students. However, PEC was informed that on August 29, 2024, FBCS filed a petition for bankruptcy in the U.S Bankruptcy Court for the Eastern District of Pennsylvania and would no longer be handling notifications on PEC’s behalf. PEC has undertaken notification of additional individuals identified by FBCS as being potentially affected by the incident

II. Number of Residents Notified

The number of notified Maryland residents whose personal information could be affected is 1. Based on information provided to PEC by FBCS, the categories of information impacted by the incident include some combination of: first and last name, address, social security number, date of birth, email address, phone number, collection account number, and driver’s license. Notices to Maryland residents began to be sent on September 6, 2024. Written notice was provided in substantially the same form as the letter attached here as **Exhibit A**.

III. Steps Taken to Address the Incident

PEC is providing impacted individuals access to credit monitoring services for 1 year to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

PEC is also providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card and/or bank. PEC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Sincerely,



Greg Jansen
Senior Vice President, General Counsel and Corporate Secretary
Perdoceo Education Corporation
1750 E Golf Rd, Suite 350
Schaumburg, IL 60173
(847) 781-3600

EXHIBIT A

WRITTEN NOTICE

Notice of Data << Event/Breach>>

Dear <<Name 1>>:

Financial Business and Consumer Solutions, Inc. (“FBCS”), a vendor of <<Data Owner>> engaged to perform certain debt collection services on our behalf, was recently the target of a cybersecurity event in which personal information for some of our <<current and former/former>> students may have been impacted. We’re sorry that this happened and regret the need to let you know about the incident. We value the trust you place in us and take safeguarding personal information seriously.

This letter provides details of the incident and the resources available to you to help protect your information should you feel it is appropriate to do so.

What Happened? On February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. This incident did not impact computer systems outside of FBCS’s network, including any systems belonging to <<Data Owner>>. FBCS immediately took steps to secure the impacted environment and launched an investigation with the assistance of third-party computer forensics specialists to determine the full nature and scope of the incident. The investigation determined that the environment was subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access, including information held on behalf of <<Data Owner>>. We are notifying you because certain information related to you may have been accessed or exfiltrated during this incident. This notification was not delayed as a result of a law enforcement investigation.

What Information Was Involved? As indicated to us by FBCS, the types of information potentially affected by this incident include your: <<Breached Elements>>. At this time, <<Data Owner>> has no indication that your information has been misused in relation to this event.

What We Are Doing. We are offering you access to complimentary credit monitoring and identity restoration services for <<12/24>> months through CyEx. Please review the attached *Steps You Can Take to Help Protect Your Personal Information* for instructions regarding how to enroll and for additional information regarding these services. Please note you will need to enroll yourself in these services if you wish to do so, as we are not able to activate the services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Your Personal Information*. In addition, we encourage you to remain vigilant against incidents of identity theft and fraud, to monitor your account statements to detect errors, and to review your credit reports for suspicious activity. We also encourage you to enroll in the complimentary credit monitoring services we are offering you.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 888-608-7439, Monday through Friday, 9AM – 9PM Eastern Time.

Sincerely,
<<Data Owner>>

Steps You Can Take to Help Protect Your Personal Information

Enroll in Credit Monitoring



Identity Defense

<<Name 1>>

Enter your Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Service Term: <<12/24>> Months*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/cec

- 1. Enter your unique Activation Code <<Activation Code>>**
Enter your Activation Code and click 'Redeem Code'.
- 2. Create Your Account**
Enter your email address, create your password, and click 'Create Account'.
- 3. Register**
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
- 4. Complete Activation**
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether you make the request online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554 Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160 Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and <https://oag.dc.gov>.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and <https://www.ncdoj.gov>.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; <https://www.riag.ri.gov>; and 1-401-274-4400. Under Rhode Island law, individuals have the right to file or obtain any police report filed in regard to this event. There is/are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.