



**CCBC**  
Community College  
of Baltimore County

**443-840-CCBC** (2222)

**CCBC Catonsville**  
800 South Rolling Road  
Baltimore, Maryland  
21228

**CCBC Dundalk**  
7200 Sollers Point Road  
Baltimore, Maryland  
21222

**CCBC Essex**  
7201 Rossville Boulevard  
Baltimore, Maryland  
21237

**CCBC Hunt Valley**  
11101 McCormick Road  
Suite 100  
Hunt Valley, Maryland  
21031

**CCBC Owings Mills**  
10300 Grand Central Avenue  
Owings Mills, Maryland  
21117

**CCBC Randallstown  
at The Liberty Center**  
3637 Offutt Road  
Randallstown, Maryland  
21133

*The incredible value  
of education.*

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

September 3, 2024

**VIA US MAIL AND EMAIL to [Idtheft@oag.state.md.us](mailto:Idtheft@oag.state.md.us)**

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

Ladies and Gentlemen

Pursuant to the Personal Information Protection Act (PIPA), Md. Code Ann. Comm. Law §14-3504, I am writing on behalf of the Community College of Baltimore County ("CCBC") to provide notice that PII relating to a single student was inadvertently disclosed to thirty-nine prospective students due to the error of an employee.

**What happened?** CCBC discovered on August 29, 2024 that emails sent by a CCBC employee to thirty-nine prospective students informing them of an upcoming orientation, inadvertently included as an attachment thereto the completed application of another student (the "Affected Student") containing her personal identifying information, instead of a blank application form that the sender intended to attach. This was a limited disclosure based on a single employee's error. The PII disclosed included the Affected Student's social security number, date of birth, phone number, mailing address, email address, demographic and household information and income.

**What did CCBC do in response?** Prompt efforts were made to recall those thirty-nine emails. The attached notice to the Affected Student was prepared with respect to the inadvertent disclosure of the Affected Student's application, containing:

- A description of the information compromised;
- Contact information for CCBC's IT Security Administrator;
- Toll-free numbers and addresses for the three credit reporting agencies: Equifax, Experian, and TransUnion;
- Toll-free numbers, addresses, and websites for the Federal Trade Commission and the Maryland Office of the Attorney General;
- A statement that the Affected Student can obtain information from these sources about steps to avoid identity theft; and
- An offer to provide three years of credit monitoring and identity protection for the Affected Student, at her option. at CCBC's cost.

In addition, CCBC has notified all recipients of the email containing the Affected Student's application to destroy the email and its attachment, and not to convey, use, disclose or transmit it to others. CCBC is also undertaking steps to prevent reoccurrence of this kind of employee error and has counselled the employee responsible. Should you require additional information relating to this notice, please contact me at the number below.

Sincerely,

***Virginia Barnhart***

Virginia W. Barnhart, Assistant General Counsel

---

**Virginia W. Barnhart, Asst. General Counsel, Community College of Baltimore County**  
7200 Sollers Point Rd, Baltimore, MD 21222 / [vbarnhart@ccbcmd.edu](mailto:vbarnhart@ccbcmd.edu) / (410) 967-5561

---



**CCBC**  
Community College  
of Baltimore County

**443-840-CCBC** (2222)

**CCBC Catonsville**  
800 South Rolling Road  
Baltimore, Maryland  
21228

**CCBC Dundalk**  
7200 Sollers Point Road  
Baltimore, Maryland  
21222

**CCBC Essex**  
7201 Rossville Boulevard  
Baltimore, Maryland  
21237

**CCBC Hunt Valley**  
11101 McCormick Road  
Suite 100  
Hunt Valley, Maryland  
21031

**CCBC Owings Mills**  
10300 Grand Central Avenue  
Owings Mills, Maryland  
21117

**CCBC Randallstown  
at The Liberty Center**  
3637 Offutt Road  
Randallstown, Maryland  
21133

*The incredible value  
of education.*

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

VIA US MAIL AND EMAIL to (Affected Student Email Address]

[Affected Student Name]

[Affected Student Mailing Address]

Dear [Affected Student]:

We are writing to inform you of the inadvertent disclosure of personal information you provided to CCBC in your prior application to the CNA program.

**What happened?** CCBC discovered on August 30, 2024 that a copy of your prior application to the CNA program was inadvertently emailed on August 28, 2024 to a group of 39 prospective students. The sender intended to include a blank application packet, but instead erroneously included a copy of your prior application form, which contained personal identifying information concerning you.

**What did CCBC do in response?** Once CCBC discovered this error, prompt efforts were made to recall those emails. We are in the process of contacting all individuals to whom those emails were sent, directing them to destroy them and the copy of your application, and to neither use, nor disseminate, the information contained therein. The College has also taken steps to prevent this incident from occurring again and is dedicated to ensuring the integrity of student data.

**What information was involved?** Your name, birth date, social security number, phone number, mailing and email addresses, demographic, household and income information were included in the copy of your CNA application that was inadvertently emailed to 39 recipients as reflected above.

We apologize for any concern this has caused you. To help ameliorate this concern, the College is willing to pay for three years of credit monitoring and identity theft protection for you. Next week you will receive a notice of how to enroll in that protection, at your election, with a link to do so free of charge.

**What you can do?** In addition to enrolling in the credit monitoring and identity theft protection you will receive notice of next week, we encourage you to remain vigilant by reviewing your account statements, monitoring your free credit reports for suspicious activity, protecting your passwords and changing them regularly, and utilizing dual authentication on your financial accounts. We also have included some additional steps that you can take to protect yourself on the attachment to this letter, as you deem appropriate.

**For more information about this notice,** you may email our data security response team at [Information-Safety@ccbcmd.edu](mailto:Information-Safety@ccbcmd.edu) or call 443-840-4001 between 8:00 am - 5:00 pm EST Monday - Friday (excluding holidays).

Sincerely,

***Suzette Fedd***

Suzette Fedd, Administrator, IT Security  
Community College of Baltimore County

## **ADDITIONAL STEPS YOU MAY WISH TO TAKE**

Below is information on additional steps you can take to protect yourself, if you feel it necessary.

➤ **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and 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. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

➤ **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

➤ **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank

accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 877-322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the 3 credit reporting agencies directly to obtain such additional reports.) –

- Equifax, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- Experian, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

➤ **POLICE REPORT:** If you are an identity theft victim, you have the right to file a police report and obtain a copy of it.

➤ **FAIR CREDIT REPORTING ACT (FCRA):** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit “prescreened” offers of credit and insurance you get based on information in your credit report. 10) You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. 11) You may seek damages from violators. 12) Identity theft victims and active duty military personnel have additional rights.

➤ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html>. Federal Trade Commission also provides information at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

➤ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM YOUR STATE ATTORNEY GENERAL.**

- You may contact and obtain information from your state attorney general at: Maryland Attorney General’s Office, 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662; [www.oag.state.md.us](http://www.oag.state.md.us) Consumer Hotline 1-410-528-8662, or [consumer@oag.state.md.us](mailto:consumer@oag.state.md.us).