



McNees Wallace & Nurick LLC
100 Pine Street
P.O. Box 1166
Harrisburg, PA 17108-1166

Christian Wolgemuth
Direct Dial: 717.237.5371
Fax: 717.237.5300
cwolgemuth@mcneeslaw.com

November 21, 2023

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
ldtheft@oag.state.md.us
200 St. Paul Place
Baltimore, MD 21202

SUBJECT: Brodart Co.
RE: Notice of Data Breach

To Whom it May Concern:

Pursuant to the Personal Information Protection Act ("PIPA"), Md. Code Ann. Comm. Law 14-3504, we are writing to notify you that our client, Brodart Co. ("Brodart"), has recently suffered a data breach.

On October 14, 2023, Brodart began experiencing an outage of its websites and its server-based IT and business systems. With the help of cybersecurity experts, Brodart has since confirmed the outage was the result of a malware-related data security attack by unauthorized third parties. Brodart personnel quickly worked to identify the issue, mitigate any additional security risks, and began the process of restoring systems to operation. In coordination with legal counsel, Brodart engaged a leading cybersecurity firm to assist them, notified law enforcement, and has been working to identify any personal information that may have been included in the data that was accessed during the incident.

Based on their investigation, Brodart has confirmed that certain personal information was accessed during this incident. This may include individuals' names, addresses, Social Security numbers, dates of birth, driver's license numbers, and in a limited number of cases, medical information, as well as financial information, such as payment card numbers, financial account numbers, and passwords.

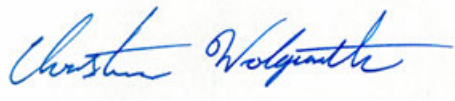
At this time, approximately 20 Maryland residents are believed to have been impacted by this incident.

Brodart is deeply committed to safeguarding the information it maintains. Upon learning of the incident, Brodart immediately enlisted the expertise of a respected third-party cybersecurity firm to implement additional best-in-class tools to further fortify their overall security posture. Brodart's commitment to ensuring the security of both data and systems is of paramount importance to them.

A copy of the notification letter sent to Maryland residents, including a complimentary offer for 1 year of free credit monitoring and fraud protection tools, is attached hereto for your reference.

Office of Attorney General
November 21, 2023
Page 2

Sincerely,

A handwritten signature in blue ink, reading "Christian Wolgemuth". The signature is fluid and cursive, with a long horizontal stroke extending from the end of the name.

Christian Wolgemuth
MCNEES WALLACE & NURICK LLC

Brodart
Mail Handling Services
777 E. Park Dr.
Harrisburg, PA 17111



[REDACTED]
[REDACTED]
[REDACTED] A-1

November 22, 2023

Dear [REDACTED]:

NOTIFICATION OF DATA BREACH

For nearly 85 years, Brodart Co. has been synonymous with world-class library products and services – a reputation that has been built by generations of dedicated employees like you. Whether you are a current Brodart team member or a former colleague from years past, and whether you worked for Brodart or one of our former affiliate companies (Tura, CRS, J.K. Gill, or Stacey's), you know that we are passionate about what we do, and we take incredible pride in our ability to provide customized and personalized solutions to our customers' needs.

Unfortunately, our company has been experiencing technical issues with our website and other business systems, which created operational challenges for us. We have continued to serve our customers throughout this incident as we investigated the cause. Through that investigation, we have recently confirmed that this incident involved a breach of data security that impacted our systems. We are writing to you today to notify you of this incident, which may have involved your personal information. While we are still investigating the incident, we felt it was important to inform you of it now so that you can take appropriate precautions to protect your interests.

What happened?

On October 14, 2023, Brodart began experiencing an outage of our websites and our server-based IT and business systems. With the help of cybersecurity experts, we have since confirmed the outage was the result of a malware-related data security attack by unauthorized third parties. We quickly worked to identify the issue, mitigate any additional security risks and began the process of restoring systems to operation. We engaged a leading cybersecurity firm to assist us, notified law enforcement and have been working to identify any personal information that may have been included in the data that was accessed during the incident.

Unfortunately, despite our efforts, we have been unable to prevent the risk of further disclosure of the inappropriately accessed data. On October 31, 2023, we were notified that a portion of the data had been disclosed on the internet by the unauthorized third parties. On November 1, 2023, we learned that some personal information of employees was included within the data accessed and disclosed by the unauthorized third parties. For this reason, we are issuing this notification to alert you that some of your personal information may have been accessed and then further disclosed by unauthorized third parties during this incident.

What information was involved?

Based on our investigation, we have confirmed that certain personal and financial information was accessed during this incident. This may include individuals' names, addresses and Social Security numbers, date of birth, driver's license number, and in a limited number of cases, medical information, as well as financial information, such as payment card numbers, financial account numbers, and passwords. Our investigation is ongoing, and therefore we are unable to provide you with a specific list of what – if any – of your specific personal or financial information may have been involved.

What are we doing?

We are deeply committed to safeguarding the information we maintain. Upon learning of the incident, we immediately enlisted the expertise of a respected third-party cybersecurity firm to mitigate the incident and implement additional best-in-class tools to further fortify our overall security posture, including enhancing our anti-intrusion measures and anti-virus protection tools. Our commitment to ensuring the security of both data and systems is of paramount importance to us.

However, we recognize you may have concerns regarding any of your information that may have been involved in this incident. To help ease those concerns, we are offering a complimentary one-year membership to Experian IdentityWorksSM. This includes 12 months of credit monitoring and fraud detection tools. In addition, the membership includes \$1 million in identity theft insurance* and identity restoration services, should you become a victim of identity theft. To activate these services, please refer to the attached document.

What can you do?

We recommend that you review your credit card and bank information, including your statements and charges. If you believe there is an unauthorized charge on your payment card, please notify the relevant payment card company by calling the number on the back of the card. Under federal law and card company rules, customers who notify their payment card company in a timely manner upon discovering fraudulent charges will not be responsible for those charges.

Please also review the attachments to this letter, titled *Steps You Can Take to Help Protect Your Information*, and *How to Enroll in Credit Monitoring and Identity Theft Protection Services* for further information on how to receive free credit monitoring/identity theft protection services for one year and how to order a free credit report.

Our Commitment to You

We take the security of your data very seriously. That is why we wanted to promptly notify you of this incident, explain what we have done in response and reassure you that our new and upgraded systems are safe. If you have additional questions or need further information, please call us at 1-800- 426-5298, Monday through Friday 8:00 am to 5:00 pm Eastern Time.

Thank you.

Sincerely,

A handwritten signature in dark ink, reading "George F. Coe". The signature is fluid and cursive, with the first name "George" being the most prominent.

George F. Coe President & CEO
Brodart Co.

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Steps You Can Take to Help Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to [IdentityTheft.gov](https://www.ftc.gov/) or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. The FTC can also provide you with additional information on how to safeguard your identity at their website, <https://www.ftc.gov/>. You can reach the FTC by phone at (202) 326-2222, or by mail at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Obtain and Monitor Your Credit Report

You may also choose to order a free credit report. If you are a U.S. resident, federal law gives you the right to obtain a free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete an Annual Credit Report Request Form and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request format: <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax

(888) 378-4329
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian

(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion

(800) 916-8800
www.transunion.com
1510 Chester Pike Crum
Lynne, PA 19022

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze

In some U.S. states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

In addition, if you are a resident of Maryland you can contact the Maryland Office of the Attorney General for more information and assistance at <https://www.marylandattorneygeneral.gov/>, 1-888-743-0023, 200 St. Paul Place, Baltimore, MD 21202; if you are a resident of North Carolina you can contact the North Carolina Office of the Attorney General for more information and assistance at <https://ncdoj.gov/>, (919) 716-6400, 9001 Mail Service Center Raleigh, NC 27699-9001; if you are a resident of New York you can contact the New York Office of the Attorney General for more information and assistance at <https://ag.ny.gov/>, 1-800-771-7755, Office of the New York State Attorney General, The Capitol, Albany NY 12224-0341; if you are a resident of Rhode Island you can contact the Rhode Island office of the Attorney General for more information and assistance at <https://riag.ri.gov/>, (401) 274-4400, RI Office of the Attorney General, 150 South Main Street, Providence, RI 02903; and, if you are a resident of the District of Columbia you may contact the Office of the DC Attorney General at <https://oag.dc.gov/about-oag/contact-us>, (202) 727-3400, 400 6th Street NW, Washington, D.C. 20001.

Credit Monitoring & Identity Theft Protection Services

Brodart has arranged with Experian IdentityWorksSM to provide you with credit monitoring/identity theft protection services for one year, at no cost to you. For more information on this complimentary service, please refer to the attachment, titled *How to Enroll in Credit Monitoring and Identity Theft Protection Services*.

How to Enroll in Credit Monitoring and Identity Theft Protection Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: 2/29/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by **2/29/2024**. Be prepared to provide engagement number **B109528** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.

- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.