Bellingham Public Library

07/21/2022

«NameFirst» «NameLast»
«Address_1»
«Address_2»
«City», «State» «Zip»

Re: Data Security Breach Notification

Dear «NameFirst» «NameLast»,

I am writing to notify you of a third-party security incident that may affect the privacy of your personal information.

WHAT HAPPENED?

On July 11, 2022, Whatcom County Library System (WCLS) notified the Bellingham Public Library (BPL) of a security incident that affected some BPL patron data. As outlined in the notification from WCLS, a file containing some BPL patron data was downloaded from WCLS's computer network without authorization on June 26, 2022. No data was downloaded directly from BPL or City of Bellingham computer systems.

BPL'S RELATIONSHIP WITH WCLS

Bellingham Public Library (BPL) serves residents within the city limits of Bellingham and Whatcom County Library System (WCLS) serves residents outside the city limits of Bellingham. Bellingham Public Library and Whatcom County Library System share a library catalog and electronic management system through a longstanding contract.

WHAT INFORMATION WAS INVOLVED?

The data downloaded during the incident included your full name, date of birth, library barcode number (library card number), and library Password/PIN. Although the investigation is ongoing, we have no reason to believe any additional patron data has been exposed.

BPL only collects the essential information needed to provide services. We do **not** store other highly sensitive patron information, such as credit card information, social security numbers, or additional financial information.

WHAT WE ARE DOING

To protect the confidentiality and integrity of your library service account, BPL deactivated your old Password/PIN, and you will need to reset it. Please see *Setting a New Library Password/PIN* below for more information.

We are working closely with WCLS to understand how this incident occurred. WCLS has also informed us that they are working diligently to put additional measures in place to safeguard patron information and information systems.

SETTING A NEW LIBRARY PASSWORD/PIN

Because we have deactivated the Password/PIN of patrons affected by this incident, you will need to set a new library Password/PIN online by following these steps:

1. Visit https://bellinghampubliclibrary.org/pin
2. Enter your barcode number (library card number).
3. We will email you a confirmation link with further instructions. When received, click the link, and enter a new Password/PIN. We recommend setting a unique Password/PIN different from the previous one to keep your account safe.

If you do not have an email address on file or prefer to update your Password/PIN by phone, please contact the Help Desk at the BPL, at the number listed below.

WHAT YOU CAN DO

Although we have no evidence that your information has been misused, we encourage you to remain vigilant against identity theft and fraud by regularly reviewing your various account statements and free credit reports for suspicious activity or errors. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Personal Information*.

We take this incident and patron information confidentiality, security, and privacy very seriously. Based on our ongoing commitment to keeping patron data safe, we are reviewing and enhancing our security policies, procedures, and data sharing agreements with other libraries and service providers. We are also working closely with WCLS to evaluate additional measures to help protect against future incidents affecting our shared systems.

For assistance resetting your Password/PIN, please contact the BPL Help Desk at (360) 778-7323 between the hours of 10 a.m. - 7 p.m. Monday – Thursday; and 10 a.m. - 6 p.m. Friday – Saturday.

For any other questions or concerns about this incident, please contact BPL Administration at (360) 778-7220 between the hours of 8 a.m. - 5p.m. Monday – Friday.

We apologize that this incident occurred and for any inconvenience it may have caused.

Sincerely,

Rebecca Judd
Library Director
Bellingham Public Library

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

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 some or all of the following information:

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 I.D. card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

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

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	888-397-3742	833-395-6938
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; https://consumer.ftc.gov/features/identity-theft; 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 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 and your state Attorney General.