



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

December 23, 2022

VIA E-MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent IBW Financial Corporation (“IBW”) located at 4812 Georgia Avenue NW, Washington, DC 20011, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately sixteen thousand six hundred and seventy-four (16,674) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, IBW does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 30, 2021, IBW became aware that an employee’s computer was subject to unauthorized access. IBW immediately launched an investigation with the assistance of third-party computer specialists to determine the nature scope of the event. The investigation determined that the employee’s computer was subject to unauthorized access on September 30, 2021 for a period of several minutes. During this time period, the unauthorized actor opened certain files stored on the affected computer, although the investigation was unable to determine the extent of information within each file that may have been viewed, or if any individuals’ specific information was actually viewed. Upon this discovery, IBW began a detailed review of the accessed files to determine what information was contained therein. On October 19, 2022, IBW’s review was complete, and they determined that the files contained information related to certain individuals.

The information that could have been subject to unauthorized access varies per individual but includes name Social Security number, driver's license number, financial account information, payment card information, passport number, medical information, and health insurance information.

Notice to Maryland Residents

On November 22, 2022, IBW posted notice of the incident on its website. On or about December 23, 2022, IBW provided written notice of this incident to approximately sixteen thousand six hundred and seventy-four (16,674) Maryland residents for whom it had a valid mailing address. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, IBW moved quickly to investigate and respond to the incident, assess the security of IBW's systems, and identify potentially affected individuals. IBW is also working to implement additional safeguards and training to its employees. IBW is providing access to credit monitoring services for twenty-four months through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, IBW is 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 company and/or bank. IBW 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/jpc
Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>> <<Date>>

NOTICE OF <<VARIABLE HEADER>>

Dear <<Name 1>>:

IBW Financial Corporation is writing to notify you of an incident that may affect the security of some of your information. While we are not aware of any actual or attempted misuse of your information, we are providing you with an overview of the incident, our ongoing response, and resources available to you to help protect your information, should you feel it is appropriate to do so.

What Happened? On September 30, 2021, IBW Financial Corporation became aware that an employee's computer was subject to unauthorized access. We immediately launched an investigation with the assistance of third-party computer specialists to determine the nature and scope of the event. The investigation determined that the employee's computer was subject to unauthorized access on September 30, 2021 for a period of several minutes. During this time period, the unauthorized actor opened certain files stored on the affected computer, although the investigation was unable to determine the extent of information within each file that may have been viewed, or if any individuals' specific information was actually viewed. Upon this discovery we began a detailed review of the accessed files to determine what information was contained therein. On October 19, 2022, our review was complete and we determined that the files contained information relating to certain individuals, including you.

What Information Was Involved? Although we have no evidence that your specific information was actually accessed or viewed without permission, we are providing you this notification in an abundance of caution. The following types of your information may have been affected by this incident: your name and <<Breached Elements>>.

What We Are Doing. Upon discovery of this incident, we launched an investigation with the assistance of third-party forensic investigators to determine the full nature and scope of the unauthorized activity, and worked to increase the security of our systems. As part of our ongoing commitment to the privacy of information in our care, our policies and procedures are being reviewed and enhanced where possible, additional safeguards have been implemented, and additional workforce training is being conducted to reduce the likelihood of a similar event in the future.

As an added precaution, we are also offering you twenty-four (24) months of complimentary access to credit monitoring services through Epiq. Individuals who wish to receive these services must enroll by following the enrollment instructions found in the enclosed *Steps You Can Take to Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. You may also review the enclosed *Steps You Can Take To Protect Personal Information* for additional guidance to better protect against the possibility of identity theft and fraud. We also encourage you to enroll in the complimentary credit monitoring services we are offering you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have questions or need assistance, please call 877-642-8901 Monday through Friday from 9:00 am to 9:00 pm EST.

Sincerely,

Thomas McLaurin

Thomas McLaurin, EVP/Chief Operating Officer

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

Go to www.equifax.com/activate

Enter your unique Activation Code of <<Enrollment Code>> then click “Submit” and follow these 4 steps:

1. Register:

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. Create Account:

Enter your email address, create a password, and accept the terms of use.

3. Verify Identity:

To enroll in your product, we will ask you to complete our identity verification process.

4. Checkout:

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

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 credit 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. 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 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	1-833-395-6938
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; 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 and obtain a copy of the report. 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 and your state Attorney General. 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, DC 20001; 202-727-3400; and 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 www.oag.state.md.us. IBW Financial Corporation is located at 4812 Georgia Avenue NW, Washington DC 20011.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting 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 www.ncdoj.gov.

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