

# **EXHIBIT 1**

This notice may be supplemented with any new significant facts learned after its submission. By providing this notice, Encova does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

### **Nature of the Data Incident**

The affiliated companies of Encova Mutual Insurance Group (“Encova”) utilize United Bank for certain banking and payment processing services. At the time the incident occurred, United Bank utilized a third-party software tool developed by Progress Software (i.e., MOVEit) for the secure transmission of documents. On June 30, 2023, United Bank reported to Encova that certain Encova data may have been copied without authorization from United Bank’s MOVEit application in connection with a zero-day vulnerability exploited within the MOVEit application on or around May 30, 2023. Encova promptly conducted a detailed review of the data that United Bank identified as potentially involved to determine the types of information present and to whom it related. The review, which Encova recently completed, revealed that certain personal information of certain Maine residents may have been affected.

### **Notice to Maine Residents**

On August 24, 2023, Encova provided written notice of this incident to seven (7) Maine residents. Written notice is being provided in substantially the same form as the letter included herewith as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

Encova is working with United Bank to evaluate its implementation of appropriate measures and safeguards in response to this incident. Encova is also notifying the potentially affected Maine residents and providing the residents with access to complimentary credit monitoring services through Equifax. Additionally, Encova is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud, including 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 against 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 instances of identity theft and fraud.

Please note that this notification is being submitted by Encova’s external data privacy counsel, Mullen Coughlin, LLC. Please do not hesitate to contact us via the contact information submitted herewith, should you have questions or require additional information.

# **EXHIBIT A**



Secure Processing Center  
P.O. Box 3826  
Suwanee, GA 30024

<<Name 1>>  
<<Address 1>>  
<<Address 2>>  
<<City>>, <<State>> <<Zip>>

<<Date>>

## NOTICE OF DATA INCIDENT

Dear <<Name 1>>:

We are writing to inform you of a recent incident involving United Bank, a financial institution that provides certain payment processing services for the affiliated companies of Encova Mutual Insurance Group (“Encova”). At United Bank, we take the confidentiality of our customers’ information very seriously. This notice explains the incident, complimentary services we have arranged to support you, and other steps you may wish to take to protect your personal information.

**What Happened:** We were recently informed of the compromise of MOVEit, a third-party software tool used by hundreds of companies around the world, including United Bank, to assist in the secure transfer of files. The compromise was disclosed by MOVEit’s manufacturer, Progress Software, and has been widely reported in the media to have affected a large number of companies.

**What Information Was Involved:** As a result of our investigation, we determined that on approximately May 30, 2023, an unauthorized third party obtained files that included certain personal information of some Encova policyholders. Based upon our review, we have determined that this personal information included your <<Breached Elements>>.

**What We Are Doing:** Upon learning of the incident, we immediately took measures to mitigate the impact. We took our MOVEit server offline and promptly applied all recommended remediation measures. We also launched an investigation, including with external security experts, to identify any impact on our customers. MOVEit software did not run on the bank’s core systems, which we confirmed were unaffected by the incident.

**What You Can Do:** We deeply regret that this occurred. As a precaution, we have arranged for you, at your option, to enroll in a complimentary, <<CM Duration>> credit monitoring service. We have engaged Equifax to provide you with its credit monitoring product. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. Enrolling in this program will not affect your credit score.

**This free credit monitoring service is available for you to activate until <<Enrollment Deadline>> by using the following activation code: <<Activation Code>>.** This code is unique for your use and should not be shared. Additional information about Equifax and how to enroll in this program is available in the form affixed to this letter.

You should remain vigilant for the next 12 to 24 months for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission (“FTC”) or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC’s website at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), call the FTC at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act (“FCRA”), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

**Equifax**

(800) 685-1111  
P.O. Box 740256  
Atlanta, GA 30374-0241  
[www.Equifax.com/personal/credit-report-services](http://www.Equifax.com/personal/credit-report-services)

**Experian**

(888) 397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.Experian.com/help](http://www.Experian.com/help)

**TransUnion**

(888) 909-8872  
TransUnion Fraud Victim Assistance Department  
P.O. Box 2000  
Chester, PA 19016  
[www.TransUnion.com/credit-help](http://www.TransUnion.com/credit-help)

You also have other rights under the FCRA. For further information, please visit:  
[https://files.consumerfinance.gov/f/documents/bcftp\\_consumer-rights-summary\\_2018-09.docx](https://files.consumerfinance.gov/f/documents/bcftp_consumer-rights-summary_2018-09.docx) (English)  
or [https://files.consumerfinance.gov/f/documents/bcftp\\_consumer-rights-summary\\_2018-09\\_es.docx](https://files.consumerfinance.gov/f/documents/bcftp_consumer-rights-summary_2018-09_es.docx) (Spanish).

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:

- (1) Equifax – (800) 685-1111
- (2) Experian – (888) 397-3742
- (3) TransUnion – (888) 909-8872

You will need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

*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 More Information:** We have set up a dedicated resource line to answer any questions you may have. Please do not hesitate to call **844-665-7611** if you have any questions or concerns.

All of us at United Bank deeply regret any inconvenience or concern this incident may cause and it is our priority to help you in any way we can.

Sincerely,

A handwritten signature in black ink, appearing to read "Julie R. Gurtis". The signature is fluid and cursive, with a large initial "J" and "G".

Julie R. Gurtis  
President  
United Bank



<<NAME 1>>

Enter your Activation Code: <<ACTIVATION CODE>>

Enrollment Deadline: <<ENROLLMENT DEADLINE>>

## Equifax Credit Watch™ Gold

\*Note: You must be over age 18 with a credit file to take advantage of the product

### Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications<sup>1</sup> when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts<sup>2</sup>, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock<sup>3</sup>
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft<sup>4</sup>

### Enrollment Instructions

Go to [www.equifax.com/activate](http://www.equifax.com/activate)

Enter your unique Activation Code of <<ACTIVATION 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.

<sup>1</sup>WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded.

<sup>2</sup>The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

<sup>3</sup>Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit [www.optoutprescreen.com](http://www.optoutprescreen.com)

<sup>4</sup>The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.