

# **EXHIBIT 1**

The investigation is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Happy State Bank (“HSB”) 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 Event**

On July 29, 2022, HSB became aware of unusual activity on the email account of an employee who is no longer with the company. HSB immediately launched an investigation to determine the nature and scope of the incident, which confirmed the employee was the subject of a phishing email scam. The individual’s HSB email account was accessed without authorization between July 28<sup>th</sup> and July 29<sup>th</sup>, 2022. The unauthorized activity was limited to this one email account. All HSB core banking systems were unaffected and remain secure.

The investigation was not able to confirm whether any email messages or attachments were actually accessed or viewed without authorization. Nonetheless, in an abundance of caution, HSB performed a careful review of the information contained within the account during the timeframe of the incident to identify individuals with personal information that was potentially accessible. HSB finalized this review for a portion of the potentially impacted individuals on February 7, 2023. The personal information that could have been subject to unauthorized access for this portion of the population includes the following: name, Social Security number, date of birth, and financial account number (not including security code, access code, passwords or PIN for the account).

### **Notice to Maine Resident**

On March 16, 2023, HSB provided written notice of this incident to potentially impacted individuals identified to-date, including approximately one (1) Maine resident. 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, HSB moved quickly to investigate and respond to the incident, assess and strengthen the security of HSB’s email environment, and identify the potentially affected individual. Further, HSB notified federal law enforcement regarding the event. HSB is also working to implement additional safeguards and training to its employees. HSB is providing access to credit monitoring services for twelve (12) months, through Equifax, to the individual whose personal information was potentially affected by this incident, at no cost to this individual.

Additionally, HSB is providing the impacted individual with guidance on how to better protect against identity theft and fraud, including advising the individual to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. HSB is providing the individual 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.

HSB is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

# **EXHIBIT A**



Return Mail Processing Center  
PO 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 <<VAR DATA 2 – VARIABLE HEADER>>**

Dear <<Name>>:

Happy State Bank (“HSB”) is writing to inform you of an incident that may affect the security of some of your data. This notice provides information about the incident, our response, and resources available to you to help protect your information should you feel it necessary to do so.

**What Happened?** In July 2022, we became aware of unusual activity on the email account of an employee who is no longer with the company. We immediately began a review of the matter, which confirmed the employee was the subject of a phishing email scam. The individual’s HSB email account was accessed without authorization between July 28<sup>th</sup> and 29<sup>th</sup>, 2022. The unauthorized activity was limited to this one email account. All HSB core banking systems were unaffected and remain secure.

We performed a careful review and determined that data for certain individuals was stored within the account at the time. However, our investigation was not able to confirm whether any email messages or attachments were actually accessed or viewed without authorization. Therefore, we are providing you with this notice in an abundance of caution.

**What Information Was Involved?** We are not aware of any misuse of data as a result of this incident. However, HSB is notifying you out of an abundance of caution because your information was present in the employee’s email account during the period of unauthorized access. The information related to you that was stored within the email account includes the following: <<Breached Elements>>.

**What We Are Doing.** We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate, assess and strengthen the security of our email environment to respond to the incident. Our response included resetting the account password and performing a review of the affected email account. We also reported the incident to federal law enforcement. We are also offering you access to complimentary credit monitoring services for <<Var Data 3 – CM Length>> months through Equifax. These services include credit monitoring with email notifications, daily access to your Equifax credit report, WebScan notifications, automatic fraud alerts, identity restoration services, and identity theft insurance coverage. If you wish to activate these services, you may follow the instructions included 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 information contained in the enclosed *Steps You Can Take to Protect Personal Information*. There you will also find more information about the credit monitoring services we are making available to you. While HSB will cover the cost of these services, you will need to complete the activation process to take advantage of these services.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 1-855-675-0999 (toll free), Monday through Friday between 8:00 a.m. and 8:00 p.m. Central Time (excluding major U.S. holidays). Again, we take this incident and the security of personal information in our care very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Mikel Williamson  
President - Texas  
Happy State Bank | A Division of Centennial Bank

## STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

### Enroll in Credit Monitoring



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.

## **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](http://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 will need to provide 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 ID 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 listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
1-888-298-0045	1-888-397-3742	1-800-916-8800
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](http://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. 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 6<sup>th</sup> Street, NW, Washington, DC 20001; 202-727-3400; and [oag.dc.gov](http://oag.dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us). HSB is located at 701 S Taylor Street, Amarillo, TX 79101.

*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](http://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](http://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](http://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 #>> Rhode Island residents impacted by this incident.