EXHIBIT 1

By providing this notice, FraudWatch 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 April 11, 2022, FraudWatch experienced a security incident that affected its network systems. FraudWatch engaged leading third-party cyber-forensic specialists to assist in our investigation to determine the full nature and scope of the incident. FraudWatch, with the assistance of the forensic specialists, also conducted a thorough and time-consuming review to identify any sensitive information that may have been accessed during this event. Unfortunately, on May 8, 2022, FraudWatch received confirmation that certain files stored within its environment may have been accessed. Subsequently, an exhaustive review to determine what specific data may be at risk and to whom that information relates was conducted. On May 20, 2022, FraudWatch finalized the list of individuals affected by the incident. On August 1, 2022, FraudWatch completed the review and verification of the data. As such, FraudWatch notified individuals and relevant regulators as soon as possible.

The information that could have been subject to unauthorized access may include name and username/password.

Notice to Maine Residents

On or about September 16, 2022, FraudWatch began providing notice of this incident to all affected individuals, which includes 7 Maine residents. Notice is being provided in substantially the same form as the document attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, FraudWatch moved quickly to investigate and respond to the incident, assess the security of FraudWatch systems, and notify potentially affected individuals. FraudWatch is also working to implement additional safeguards and training to its employees.

Additionally, FraudWatch 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. FraudWatch 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. FraudWatch also notified other relevant state regulators.

EXHIBIT A

RE: NOTICE OF DATA SECURITY EVENT/DATA BREACH

Dear <<Name 1>> <<Name 2>>:

FraudWatch is notifying you of a recent incident that may impact some of your information. We are providing you with information about the incident, our response to date, and resources you can take advantage of, should you feel it is appropriate to do so.

What Happened? On or about April 11, 2022, FraudWatch identified suspicious activity related to certain FraudWatch network systems. Upon discovery, we took steps to secure the FraudWatch network and launched an investigation with leading third-party cyber-forensic specialists to determine the full nature and scope of the incident. On May 8, 2022, the investigation concluded, and we determined that certain FraudWatch systems were subject to unauthorized access on separate occasions between March 3, 2022 and April 10, 2022 as a result of this incident. On May 20, 2022, we finalized the list of individuals affected by the incident.

What Information Was Involved? With the assistance of the forensic specialists, FraudWatch conducted a thorough and time-consuming review of the impacted FraudWatch systems in order to identify information which may have been impacted as a result of this event. This review identified that certain files stored within the impacted FraudWatch systems at the time of the incident contained some of your information. This information includes your name and username/password to access our website portal called PhishPortal.

What We Are Doing. We take this incident and the security of information in our care very seriously. Upon discovery of this incident, we immediately took steps to secure the impacted systems and launched an in-depth investigation to determine the full nature and scope of this incident. We are reviewing existing security policies and implemented additional cybersecurity measures to further protect against similar incidents moving forward.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, from any source, by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You can also review the enclosed *Steps You Can Take to Help Protect Your Information* for additional actions you may take, including instructions for how to enroll in the credit monitoring and identity restoration services we are offering you, should you feel it is appropriate to do so.

For More Information. If you have questions that are not addressed in this letter, please contact our Data Protection Team by email at Privacy@FraudWatch.com.

We sincerely regret any inconvenience or concern this event may cause you.

Regards,

Trent Youl
Chief Executive Officer
FraudWatch

STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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 credit 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, military identification, 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 fraud alert or 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
888-298-0045	1-888-397-3742	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; 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.

Additionally, it is recommended that you promptly change your password and security question and answer, as applicable, or take other steps appropriate to protect the potentially accessible online account information and all other online accounts for which the same username, email address, password, and security question and answer are used.