EXHIBIT 1

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Virginia Farm Bureau® and its affiliated companies[1] (collectively "VFB") 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 or about October 11, 2022, VFB was notified by the Department of Homeland Security ("DHS") through the Cyber Security and Infrastructure Security Agency ("CISA") that CISA had received a credible tip that VFB had been compromised in at least one of the systems. VFB immediately took steps to investigate and contain this activity. The activity was limited to one workstation within the environment, which was taken out of production and disconnected from VFB's network. Furthermore, VFB disabled the impacted user account, issued a new account to the user, and had the user change their password. The workstation and the user account were not expected to store any personal information, as, per policy, sensitive information should be sent through separate secure channels. The initially identified activity did not materially impact VFB's business operations.

As part of its response to this event, VFB retained Mullen Coughlin as privacy counsel. Mullen Coughlin engaged a third-party digital forensic investigation firm on VFB's behalf to assist with containment and remediation of the incident and to conduct a legally privileged investigation to confirm the nature and scope of the unauthorized activity.

On October 16, 2022, VFB began experiencing active ransomware encryption on certain systems within its network. VFB immediately began taking systems offline in an effort to contain the spread of malware to other systems within the network. On the same day, VFB promptly notified the Federal Bureau of Investigation ("FBI") of the encryption activity.

Through its investigation, VFB determined that certain of its systems were accessible to an unknown actor between October 6, 2022 and October 16, 2022, and certain files on those systems may have been viewed or downloaded. As such, VFB, with the assistance of third-party data review specialists, conducted a time-intensive and thorough programmatic and manual review of the unstructured data which was stored on the impacted systems and determined that certain sensitive information was contained therein. Following this review, VFB conducted additional review of its records to confirm the identities and contact information for potentially affected individuals in order to provide notification. This review was recently completed.

The information that could have been subject to unauthorized access includes name, driver's license or state identification number, Social Security number, and financial account information.

Notice to Maine Residents

[1] These entities include, but are not limited to, Virginia Farm Bureau Mutual Insurance Company, Countryway Insurance Company, Employee Benefits Corporation of America, Benefit Design Group, Inc., Custom Health Care, Inc., and Virginia Farm Bureau Service Corporation – Health Care Consultants division.

On or about February 15, 2024, VFB provided written notice of this incident to four thousand three hundred twenty-one (4,321) Maine residents. 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, VFB moved quickly to investigate and respond to the incident, assess the security of VFB systems, and identify potentially affected individuals. Further, VFB notified federal law enforcement regarding the event. VFB is also working to implement additional safeguards and training to its employees. VFB is providing access to credit monitoring services for one (1) year, through CyEx, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, VFB 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. VFB 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.

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

EXHIBIT A

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

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Virginia Farm Bureau® and its affiliated companies[1] (collectively "VFB" or "We") are writing to inform you of a data security event that may involve some of your information. Our affiliated companies provide a variety of services including personal and commercial insurance as well as health insurance administration and brokerage services. We are notifying you because you or a family member has received our services or are a current or former VFB employee. This letter includes details of the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? In October of 2022, we became aware that certain of our computer servers and systems were inaccessible. We immediately took steps to contain this activity, secure our systems and report the event to federal law enforcement and government regulators. We engaged leading cyber incident response specialists to perform an investigation and determine the full nature and scope of the event.

After an extensive investigation, we determined that an unknown actor had access to a limited number of systems between October 6, 2022 and October 16, 2022, and certain files on those systems may have been viewed or downloaded. Accordingly, we undertook a comprehensive and time-intensive review of the affected files with the assistance of data review specialists, to determine if the files contained personal information. Now that the investigation is complete, we are contacting all potentially affected individuals.

What Information Was Involved? The investigation determined the following types of information related to you were present in the impacted systems: your name, <<Breached Elements>>.

What We Are Doing. We take safeguarding the privacy and security of the information in our care very seriously. Upon learning of the event, we immediately took steps to secure our systems and have implemented additional security measures to further protect data in our care. We continue to enhance these protections as appropriate as part of our ongoing commitment to data security.

As an added precaution, we are also offering you <<twelve (12)/twenty-four (24)>> months of credit monitoring and identity restoration services at no cost to you through CyEx. Enrollment instructions are enclosed with this letter.

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 credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Personal Information* for useful information on what you can do to better protect against possible misuse of information. You may also enroll in the complimentary credit monitoring services we have provided for you.

[1] These entities include, but are not limited to, Virginia Farm Bureau Mutual Insurance Company, Countryway Insurance Company, Employee Benefits Corporation of America, Benefit Design Group, Inc., Custom Health Care, Inc., and Virginia Farm Bureau Service Corporation – Health Care Consultants division.

For More Information. If you have additional questions, you may call our assistance line at 888-541-1629 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, excluding U.S. holidays. You may also write to VFB at P.O. Box 27552 Richmond, VA 23261, Attn: Safeguard.

Sincerely,

Virginia Farm Bureau

Steps You Can Take to Help Protect Personal Information

Enroll in Credit Monitoring Services

Identity Defense Complete
Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions
To enroll in Identity Defense, visit https://app.identitydefense.com/enrollment/activate/virg

1. Enter your unique Activation Code **<<Activation Code>>**

Enter your Activation Code and click 'Redeem Code'.

2. Create Your Account

Enter your email address, create your password, and click 'Create Account'.

3. Register

Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.

4. Complete Activation

Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

Monitor 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 one-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, 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
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and 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, D.C. 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 https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately <<RI #>> Rhode Island residents that may be impacted by this event.