150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

November 15, 2021

Bruce A. Radke
312-463-6211
312-819-1910
bradke@polsinelli.com

VIA E-MAIL (CONSUMER@AG.IOWA.GOV)

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319

Re: ***Notification of a Potential Data Security Incident***

Dear Madam/Sir:

We represent FCS Financial ("FCS") in connection with a recent incident that may have involved the personal information of 721 Iowa residents, and we provide this notice on behalf of FCS pursuant to Iowa Code § 715C.1-2. We will supplement this notice, if necessary, with any new, significant facts discovered subsequent to its submission. While FCS is notifying you of this incident, FCS does not waive any rights or defenses relating to the incident, this notice, or the applicability of Iowa law on personal jurisdiction.

NATURE OF THE SECURITY INCIDENT

FCS experienced a data security incident that involved some of its computer systems. A subsequent forensic investigation determined FCS was the victim of a mespinoza ransomware attack. The investigation also determined that certain documents stored within FCS' network were accessible to the unauthorized third party and taken out of FCS' network at the time of the incident. An initial review of the files believed to be involved was completed on June 16, 2021, but based on the discovery of additional involved files, FCS determined that the prudent course of action was to notify all individuals whose information could have been stored on its system. FCS then worked to put together a list of these individuals and identify addresses for them. FCS completed its review and determined the documents contained the personal information of certain Iowa residents, including, primarily their name and Social Security number, and for a much smaller subset of documents may have included their driver's license number or government-issued identification number.

Although FCS is not aware of any fraud or misuse of personal information as a result of the incident, FCS provided notice of the incident to the potentially involved individuals and arranged

for them to receive an offer of complimentary credit monitoring and identity theft protection services for the individuals.

NOTIFICATION OF THE INCIDENT

FCS provided notice of the incident to 721 potentially involved Iowa residents by First Class U.S. Mail. Letters were sent in three waves on September 17, 2021, October 28, 2021, and November 8, 2021. Enclosed is a copy of the notice that FCS sent to the involved individuals via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon discovering the incident, FCS promptly conducted an internal investigation and engaged a leading forensic firm to investigate the incident and confirm the security of FCS' computer systems and network. FCS has also undertaken efforts to reduce the risk of a similar incident occurring in the future, including enhancing its technical security measures. Finally, as discussed above, FCS provided notice of the incident to the potentially involved individuals with information on how they can protect themselves against identity theft. FCS also included an offer of twenty-four months of complimentary credit monitoring and identity theft protection services in the notification letters.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Bruce A. Radke

Enclosure

FCS FINANCIAL
Growing Relationships. Creating Opportunities.™
A FARM CREDIT COOPERATIVE

[redacted]

[redacted]

Dear [redacted],

Based on your current or previous relationship with FCS Financial ("FCS"), we are writing to advise you of a recent incident that may have involved some of your personal information. **We have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft.** Nonetheless, because your information could have been affected, we are providing you this notice with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? FCS recently experienced a data security incident that involved some of our computer systems. A subsequent forensic investigation determined that an unknown third-party acquired certain data from our systems, including documents that may have contained some of your personal information. Although we are not aware of any instances of fraud or identity theft resulting from the incident, we conducted an internal review to determine the contents of the documents accessible to the unknown third-party.

What Information Was Involved? On June 16, 2021, our investigation determined that documents the third party acquired contained personal information about a number of individuals who either worked with or for our association. Subsequently, other information received during the investigation indicated additional individuals' personal data may have been included. Out of an abundance of caution, we are providing a broad, detailed list of the information that may have been involved. The type of information differs from individual to individual, and we cannot say with certainty whether this information was accessed for any particular person. However, the involved information may include your name; address and other contact information such as email or phone number; Social Security number; driver's license number; or financial information such as account information, tax identification number, or unique IRS-related identifier. For a limited number of individuals, the incident may have also involved their date of birth, health insurance information, or medical information.

What We Are Doing? Upon learning of the incident, we promptly restored the affected systems and conducted an initial investigation into how the incident occurred and contacted the proper authorities. We also engaged a leading forensic security firm to investigate the incident and confirm the security of our systems. In addition, we have taken steps to reduce the risk of this type of incident from occurring in the future, including implementing additional technical controls.

We have chosen to do a broad notification of the security incident to alert individuals that potentially could have been involved. Although we have no evidence of your information being used for the purposes of fraud or identity theft, we are offering you a complimentary two-year membership to Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary two-year membership, please see the supplementary information provided in this letter.

What You Can Do? You can find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet. We also encourage you to activate the credit monitoring services we are providing to you.

Other Important Information: FCS is committed to the privacy and confidentiality of our customers and community members. We take our responsibility to safeguard your personal information seriously and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call [redacted] from 8:00 AM - 5:30 PM Central Time, Monday through Friday, excluding some U.S. holidays.

Sincerely,

[redacted]

[redacted]

ACTIVATING COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** two-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [redacted]
3. PROVIDE the **Activation Code:** [redacted] **. PLEASE NOTE THAT THE ACTIVATION CODE IS CASE-SENSITIVE.**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at [redacted]
or call [redacted] to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted]

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL IMPORTANT INFORMATION

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

Other Important Information: You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

This notice was not delayed by a law enforcement investigation.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

Massachusetts Residents: Massachusetts residents have the right to obtain a police report filed or file a police report in regard to a data security incident. Massachusetts residents also have the right to place a security freeze on their credit reports without charge. To place a free security freeze, please contact the above listed three major consumer reporting agencies and provide the agencies: 1) your full name; 2) Social Security number; 3) date of birth; 4) if you have moved in the past five years; 5) proof of current address such as a current utility or telephone bill; 6) a legible photocopy of a government issued identification card; and 7) if you are a victim of identity theft, include a copy of the police report, investigative report, or complaint. Massachusetts Residents can obtain more information about preventing identity theft from the Massachusetts' Attorney General's Office at: Massachusetts Office of the Attorney General, Consumer Protection Division, One Ashburton Place, Boston, MA 02108; https://www.mass.gov/orgs/office-of-attorney-general-maura-healey.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Washington, DC Residents: Washington, DC residents can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.