NELSON MULLINS

NELSON MULLINS RILEY & SCARBOROUGH LLP
ATTORNEYS AND COUNSELORS AT LAW

106 S. President St., Suite 400
Jackson, MS 39201
M: 404.322.6000 F: 404.322.6050
nelsonmullins.com

March 2, 2023

John Formella, Attorney General
Office of New Hampshire
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: *1st Franklin Financial Corporation - Notice of Data Security Incident*

Dear Attorney General Formella:

I serve as outside legal counsel to 1st Franklin Financial Corporation ("1FFC"). 1FFC is a financial services company with its principal office located at 135 E. Tugalo Street, Toccoa, GA 30577.[1]

This correspondence is to notify you of a security incident at 1FFC that occurred between November 17 – 18, 2022, involving the unauthorized encryption of certain electronic files within the company's network environment. 1FFC immediately took steps to address the situation, promptly changing passwords and blocking the unauthorized access.

Third-party forensic experts were also engaged to investigate and remediate this incident. Findings from the investigation indicate that during the incident an unauthorized third party may have accessed and/or exfiltrated data from certain file folders in 1FFC's network. On or about December 15, 2022, 1FFC determined that the potentially-impacted files may contain personally identifiable information. From there, 1FFC conducted a review of the data (which involved a combination of automated and eyes-on examination of the impacted files) to identify individuals whose personal information may have been involved. Based on the results of the investigation, on January 10, 2023, 1FFC began

[1] By providing this notice, 1FFC does not waive any rights or defenses regarding the applicability of your State's law, the applicability of your State's data event notification statute, or personal jurisdiction.

issuing notices to potentially affected individuals based on the information available at that time.

Subsequently, 1FFC continued its investigation and conducted a voluminous document review process (which involved programmatic searching and hand reviewing of individual documents) to identify additional individuals who potentially needed to be notified of this incident. After completing this arduous e-discovery process, on January 28, 2023, 1FFC was provided an updated list of potentially affected individuals, which identified residents of your state.

In an abundance of caution, 1FFC began sending notices via U.S. Mail on or about February 15, 2023, to 49 residents of your state. The notification letters include instructions for activating credit monitoring services at no cost to the recipients. The PII that was potentially at risk included first and last names, social security number, bank account number and routing information if the consumer provided that information to 1FFC for ACH transfers or via a check, and potentially information contained in a credit report for the consumer. Sample notification letters are enclosed for your reference and include:

- A description of the security event;
- Steps taken to investigate;
- Steps taken to mitigate any potential harm to consumers;
- Instructions for activating free identity theft protection services that include credit monitoring and a $1 million insurance reimbursement policy to all consumers who received notification;
- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this event, etc.

1FFC is fully committed to protecting consumer privacy and the confidentiality of personal information. Since the investigation remains ongoing, we may supplement this notice if necessary. Please contact me if you require any additional information regarding this incident.

Best regards,

Brad C. Moody

Enclosures:
See attached for sample Notification Letters

1st Franklin Financial

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

This date contains a typo as it should read as "January 10, 2023".

February 14, 2023

Dear [redacted]

On behalf of 1st Franklin Financial Corporation ("1FFC"), I am writing to notify you of a recent incident that may have involved some of your personal information.

What happened and what have we done in response? On or about November 17, 2022, we sustained a security incident, causing disruption to our information technology network. We immediately investigated and aggressively responded to this event. Passwords were changed, and the unauthorized access was blocked. Outside technical experts were also engaged to further investigate and evaluate the nature and scope of the incident.

What information was involved? Preliminary findings from the investigation indicate that during the incident an unauthorized third party may have accessed and/or exfiltrated some data from 1FFC's IT environment. In response, we conducted a review of the data (which involved a combination of automated and eyes-on examination of the impacted files) to identify individuals whose personal information may have been involved. Through this review, we determined that some personal information in our files may have been impacted.

On January 10, 2022, 1FFC began issuing notices to potentially affected individuals based on the information available at that time. As our investigation continued, we identified additional potentially-impacted files that may have contained your first and last names, social security number, bank account number and routing information if you provided that information to 1FFC for ACH transfers or via a check, and potentially information contained in a credit report for you. The exact data elements that were impacted by the event varied by individual. **We do not have any evidence that anyone has actually misused your information but are notifying you out of an abundance of caution.**

What can you do? We recommend you take precautions, and we are offering you 12 months of **free** credit monitoring and $1 million in identity theft insurance through Experian. **You must activate the Experian product by the activation date for it to be effective. The activation instructions are included with this notification.** We also have enclosed some additional steps that you can take to protect yourself, as you deem appropriate.

For more information about this incident, please call (866) 982-6335 Monday through Friday, from 9:00 am -6:00 pm (excluding major U.S. holidays). We take information privacy and security issues very seriously and are continuing to take steps to enhance our security measures to help reduce the risk of something like this happening in the future. We are fully committed to protecting your personal information and sincerely apologize for any concern this incident may have caused.

Sincerely,

Ginger Herring
President & CEO
1st Franklin Financial Corporation

Steps You Can Take:

Below is information on steps you can take to protect yourself, if you feel necessary.

➢ **ACTIVATE Your FREE Experian IdentityWorks Product NOW in Three Easy Steps.** To help protect your identity, we are offering you a **complimentary** 12 **month membership** to Experian's IdentityWorks product. This product helps detect possible future misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks Alert is completely free to you and enrolling in this program will not hurt your credit score.

1. **ENSURE You Enroll By: 05/06/2023 (Your code will not work after this date.)**
2. **VISIT** the **Experian IdentityWorks website** to enroll: https://www.experianidworks.com/3bcredit
3. **PROVIDE Your Activation Code:** [redacted]

If you have questions about the IdentityWorks or need an alternative to enrolling online, **please call 800-459-4631** and provide engagement [redacted]. A credit card is not required for enrollment. Once your IdentityWorks membership is activated, you will receive the following features:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only[1].
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Restoration Agents are immediately available to help address credit/non-credit related fraud.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

You must activate your membership by the Enrollment Date (noted above) by enrolling at https://www.experianidworks.com/3bcredit or calling 800-459-4631 to register your activation code above in order for this service to be activated. Once your enrollment in IdentityWorks is complete, carefully review your credit report for inaccurate or suspicious items. 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 team at 800-459-4631.

Additional Steps You May Wish to Take:

➢ **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

ORDER YOUR FREE ANNUAL CREDIT REPORTS. Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize.

---

[1]Offline members will be eligible to call for additional reports quarterly after enrolling.

[2]The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

➢ **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze. To place a security freeze on your credit report, contact each of the 3 major consumer reporting agencies -

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.comm	www.transunion.com

To request a freeze, you will need to provide the following:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.), Social Security Number, and Date of birth; and
- If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
- Proof of current address such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have 3 business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

➢ **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.

➢ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC.** You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies or the Federal Trade Commission. Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html. Federal Trade Commission also provides information at www.ftc.gov/idtheft FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

➢ **FILE YOUR TAXES QUICKLY AND SUBMIT IRS FORM 14039.** If you believe you are at risk for taxpayer refund fraud, the IRS suggests you file your income taxes quickly. Additionally, if you are an actual or potential victim of identity theft, the IRS suggests you give them notice by submitting IRS Form 14039 (Identity Theft Affidavit). This form will allow the IRS to flag your taxpayer account to alert them of any suspicious activity. Form 14039 may be found at https://www.irs.gov/pub/irs-pdf/f14039.pdf.

➢ **FAIR CREDIT REPORTING ACT:** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Note - Identity theft victims and active duty military personnel have additional rights.

➢ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM YOUR STATE ATTORNEY GENERAL.**

- *Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662; www.oag.state.md.us Consumer Hotline1-410-528-8662, or consumer@oag.state.md.us.*
- *Connecticut: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag*
- *District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, databreach@dc.gov, www.oag.dc.gov.*
- *Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html*
- *New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-6971220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov*
- *North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6000/ 1-877-566-7226, www.ncdoj.gov*
- *Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov. (Approximately 22 Rhode Island residents were impacted by this incident.)*