Clark Hill

Jason M. Schwent
T (312) 985-5939
F (312) 517-7573
Email:jschwent@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

September 16, 2022

Via Portal

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Dear Attorney General Frey:

We represent Berry, Dunn, McNeil & Parker ("BerryDunn") as outside counsel with respect to a data security incident involving personal information as described below. BerryDunn, headquartered in Maine, is notifying you of this incident on behalf of its clients, who are the owners of the impacted data. (See Exhibit A).

1. Nature of security incident.

On June 8, 2022, BerryDunn received reports from some clients about unusual emails that were received from what appeared to be a BerryDunn email account. BerryDunn immediately investigated the unusual activity, implemented its incident response protocols, and determined that the emails originated from an account outside of the organization. BerryDunn also hired external computer forensic specialists to determine what occurred and what data may have been impacted. The forensic specialists reported findings to BerryDunn on August 1, 2022. The investigation found that there had been unauthorized access to one employee's email account. The investigation, however, could not determine whether materials within that email account may have been accessed. As part of the investigation, the external forensic specialists conducted a review of the contents of the email account to determine what information may have been in the account at the time of the incident. Though there was no evidence of any access to or misuse of any of the information found in the affected email account, BerryDunn notified clients who had provided data to BerryDunn and worked with them to prepare notification letters, arrange for mailing, and arrange for impacted individuals to receive credit monitoring and identity restoration services.

2. Number of residents affected.

One-thousand two-hundred forty (1,240) of Maine's residents may have been affected and were notified of the incident. For those that requested BerryDunn mail letters, a letter was sent to the potentially affected individuals on September 16, 2022, via regular mail (a copy of the form

notification letter is enclosed as Exhibit B). Another mailing is expected next week to additional affected individuals pursuant to the request of some of BerryDunn's clients. Impacted information may include names, Social Security numbers, Driver's License numbers/State ID numbers, and Health Insurance Policy numbers.

3. Steps taken in response to the incident.

Since this incident, BerryDunn isolated the unauthorized access to the email account and changed the password to the affected email account. Additionally, impacted individuals were offered 24 months of credit monitoring and identity protection services through IDX.

4. Contact information.

BerryDunn takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

Jason M. Schwent
Senior Counsel

cc: Mariah Leffingwell – mleffingwell@clarkhill.com

EXHIBIT A

Entity	Number of Individuals Affected
Kennebec Savings Bank	207
Northern Maine Medical Center	316
Spurwink Services, Inc.	281
Stone Coast Fund Services LLC	188
Woodard & Curran, Inc.	248

EXHIBIT B

Berry, Dunn, McNeil & Parker, LLC
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 764-2896
Or Visit:
https://response.idx.us/bdmp
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

September 16, 2022

Notice of Data <<Variable Text 3>>

Dear <<First Name>> <<Last Name>>,

We are writing to let you know about a data security incident that may have impacted your personal information. Berry, Dunn, McNeil & Parker, LLC ("Berry Dunn") provides accounting and auditing services to customers. We may have your information if <<Variable Text 1>> provided your information to us in the course of obtaining our services. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened?

On June 8, 2022, we received reports from some of our clients about unusual emails that they received from what appeared to be a BerryDunn email account. We immediately investigated the unusual activity, implemented our incident response protocols, and determined that these emails originated from an account outside our organization. We also hired external computer forensic specialists to determine what occurred and what data may have been impacted. The investigation found that there had been unauthorized access to one employee's email account. These forensic specialists reported findings to us on August 1, 2022. As part of the inquiry, the external forensic specialists conducted a review of the contents of that email account to determine what information may have been affected. The investigation found that information provided to us by <<Variable Text 1>> was located within the affected email account. While there is no evidence that any of your information was viewed, copied, removed, or otherwise accessed by unauthorized actors we wanted to inform you of this incident out of an abundance of caution.

What Information Was Involved?

Your information that was found to be present in the email account at the time of the account includes your name and the following data elements: <<Variable Text 2>>.

What We Are Doing:

Data security is one of our highest priorities. We want to assure you that we are taking steps to prevent a similar incident from happening in the future. Upon initial investigation, we isolated the unauthorized access to one account and reset the user's credentials.

In addition, we are offering identity theft protection services through IDX the data breach and recovery services expert, at no charge to you. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a

$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

It is always a good idea to review your credit reports, bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (833) 764-2896 or going to https://response.idx.us/bdmp and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is December 16, 2022. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information:

If you have any questions or concerns, please call (833) 764-2896 Monday through Friday from 9 am - 9 pm Eastern Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Clare E. Lizotte, Esq.
Berry, Dunn, McNeil & Parker, LLC

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to **https://response.idx.us/bdmp** and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 764-2896 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly. You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place

the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 agencies 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 a violator. 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. You should report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400. There are 56 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.