MARSHALL DENNEHEY

Granite Square, 700 State Street, 3rd Floor
New Haven, CT 06511

Wall Street Plaza, 88 Pine Street, 21st Floor, New York, NY 10005-1801
(203)714-4560 Fax (203)714-4561

Direct Dial: (203)714-4565
Email: rdlane@mdwcg.com

March 8, 2022

Via Email: attorneygeneral@doj.nh.gov
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Porte Brown, LLC - Data Incident
Our File No. 41088.00177

Dear Sir or Madam:

We are writing to notify you of a data security incident involving 2 New Hampshire residents. We are submitting this notification on behalf of our client, Porte Brown, LLC.

Nature Of The Security Breach

Porte Brown, LLC is an accounting firm based in Illinois. In November 2020, Porte Brown was notified by Netgain, its third-party IT service provider, that Netgain was the victim of a ransomware attack, which resulted in the exposure of a limited amount of data from some of its customers. Porte Brown was among the customers affected by the incident. After a thorough forensic investigation of Porte Brown's systems, it was determined in February 2021 that approximately 10% of Porte Brown's accounting data was exposed during the Netgain breach. As a result, some of the personal information belonging to New Hampshire residents may have been exposed to others, including their names, addresses and social security numbers. However, after consultation with the FBI and cybersecurity experts, steps were taken to ensure that the data was not misused. Additionally, Porte Brown has confirmed that any unauthorized access has been stopped and that its systems are secure.

The residents involved in this incident were forwarded letters notifying them of this incident on December 20, 2021. A copy of the form letter is attached hereto.

Steps Taken Relating To The Incident

Based on the nature of the incident and the steps taken by Netgain, Porte Brown has no reason to believe that any of the data exposed was or will be misused, disseminated, or otherwise made publicly available. Upon discovering this incident, Netgain immediately secured the system. They also retained third-party forensic experts to assist in their investigation of this incident. They have also reviewed their internal data management protocols and have implemented enhanced security measures to help prevent this type of incident from recurring. They have assured Netgain of their commitment to prevent future cyber thefts.

Porte Brown, LLC has also arranged to protect the individuals affected by this incident by providing identity monitoring services for two years at no cost to the individuals.

Should you need additional information regarding this matter, please contact me.

Very truly yours,

R. David Lane, Jr.

RDL:dml
Enclosure

PorteBrown
ACCOUNTANTS & ADVISORS

Return Mail Processing
PO Box 999
Suwanee, GA 30024

December 17, 2021

40 I 11128 **********SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

NOTICE OF DATA BREACH

Dear Sample A. Sample:

Porte Brown, LLC takes the privacy and protection of your personal information very seriously. We are writing to inform you of a data privacy incident that may have involved some of your tax and accounting personal information.

What Happened
In November 2020, we were notified by Netgain, our third-party IT service provider, that they were the victim of a ransomware attack, which resulted in the exposure of a limited amount of data from some of its customers. Porte Brown was among the customers affected by the incident. After a thorough forensic investigation of Porte Brown's systems, it was determined in February 2021 that approximately 10% of Porte Brown's accounting data was exposed during the Netgain breach. However, after consultation with the FBI and cybersecurity experts, steps were taken to ensure that the data was not misused. Additionally, we have confirmed that any unauthorized access has been stopped and that our systems are secure.

What Information Was Involved
Based on our investigation, we have determined that the personal information that was potentially accessed by the third party may have included first and last names, addresses and social security numbers.

Netgain's Response
Based on the nature of the incident and the steps taken by Netgain, we have no reason to believe that any of the data exposed was or will be misused, disseminated, or otherwise made publicly available. Upon discovering this incident, they immediately secured the system. They also retained third-party forensic experts to assist in their investigation of this incident. They have also reviewed their internal data management and protocols and have implemented enhanced security measures to help prevent this type of incident from recurring. They have assured us of their commitment to prevent future cyber thefts.

What We Are Doing
While the evidence provided by Netgain indicates that the exposed data was not used maliciously, we are as concerned as you might be that the breach occurred. We have worked with additional outside IT resources to ensure the steps taken by Netgain and by ourselves have made the network as secure as possible. Based on new security software that has been added and the increased monitoring and testing that has taken place, we are confident that all the necessary steps have been taken to protect our data going forward.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for two years.
If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary two-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by February 28, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **www.experianidworks.com/credit**
- Provide your **activation code**:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 796-8638** by **February 28, 2022**. Be prepared to provide engagement number s proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR TWO-YEAR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related 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.

What You Can Do

Although according to Netgain none of the data exposed will be misused, disseminated, or otherwise made publicly available, we still recommend that you review the enclosed "Information About Identity Theft Protection" reference guide, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission. You may also take advantage of the complimentary identity protection services being offered.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or would like an alternative to enrolling online, please call (833) 796-8638 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B021232.

Sincerely,

Porte Brown, LLC

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

** 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.

Information About Identity Theft Prevention

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report once every 12 months from each of the three nationwide credit reporting agencies. To order your annual free credit report, please visit www.annualcreditreport.com, or call toll-free 1-877-322-8228. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax:	P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian:	P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion:	P.O. Box 2000, Chester, PA 19016, 1-800-888-4213, www.transunion.com

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For Connecticut residents, the Attorney General can be contacted at 55 Elm Street, Hartford, CT 06106. www.ct.gov/ag, 1-860-808-5318.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. Pristine Dental is located at 555 Providence Highway, Unit 2, Walpole, MA 02081.

For 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 violators. 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. We encourage you to review your 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 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/.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, 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 a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security 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 security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at: **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com; **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com; **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com.

To request a security freeze, you will need to provide the following information: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc.) (2) Social Security number (3) Date of birth (4) If you have moved in the past five years, provide the addresses where you have lived over the prior 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.) (7) If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five 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 in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies 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 identity 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 one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus 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 one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

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 of FCRA rights includes: (1) The right to receive a copy of your credit report that contains all the information in your file at the time of your request; (2) each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months; (3) you are also entitled to a free report if a company takes adverse action against you, like 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. (4) 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. (5) You have the right to ask for a credit score. (6) You have the right to dispute incomplete or inaccurate information. (7) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. (8) Consumer reporting agencies may not report outdated negative information. (9) Access to your file is limited. You must give your consent for reports to be provided to employers. (10) You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report. (11) You may seek damages from violators. (12) Identity theft victims and active duty military personnel have additional rights.