Debevoise & Plimpton

Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
+1 212 909 6000

By First-Class Mail

April 26, 2021

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

On behalf of NYDIG Execution LLC and NYDIG Trust Company LLC (collectively, "NYDIG"), and pursuant to N.H. Rev. Stat. Ann. § 359-C:20, this letter provides notice of a data security incident that occurred at a NYDIG vendor that potentially affects approximately 551 individuals in total, 1 of whom is a resident of New Hampshire. NYDIG is a technology and financial services firm dedicated to Bitcoin.

On April 7, 2021, LogicGate, Inc., a software vendor used by NYDIG to provide risk management solutions, first informed NYDIG that some NYDIG data stored in the LogicGate Risk Cloud environment had been accessed by an unauthorized third party. LogicGate is located at 320 W Ohio St, Suite 5E, Chicago, IL 60654. NYDIG is one of many LogicGate customers impacted by the incident, and does not appear to have been targeted. LogicGate is unable to confirm whether the NYDIG data that was stored in its cloud environment was copied or stolen, but NYDIG is operating as if all of the data that it had stored with LogicGate that was accessed by the attackers was exfiltrated.

While LogicGate's investigation is ongoing, LogicGate has determined that on February 23, 2021, an unauthorized third party accessed and decrypted a backup file stored in LogicGate's Risk Cloud environment. That backup file contained information that NYDIG uploaded to LogicGate's Risk Cloud environment, including NYDIG's customer information. NYDIG uses LogicGate to record portions of its compliance program, including customer information that is obtained in connection with onboarding new customers and counterparties.

The types of information stored on the LogicGate system that may have been compromised included: first and last names, account numbers, dates of birth, social security or tax identification numbers, bank account numbers, passport and drivers license numbers, income, net worth, residential addresses, phone numbers, email address, and employment status. We are not aware of any resulting identity theft, fraud, or financial losses to customers.

NYDIG sent an informal notice of the incident by email to potentially affected individuals for whom we had email addresses on April 9, 2021. NYDIG is also sending a

formal notice to all potentially affected individuals by mail on April 27, 2021. A sample of the notification letter is enclosed. As stated in the attached sample notice, NYDIG is offering to provide individuals with 24 months of free identity theft and credit monitoring services through Norton LifeLock.

NYDIG conducted cybersecurity diligence on LogicGate before engaging them, and again before renewing its most recent services agreement with LogicGate in June 2020. As part of that diligence, NYDIG reviewed LogicGate's Security Scorecard Summary Report (which had a rating of 93 at the time of the renewal and currently has a rating of 95), LogicGate's SOC 2 report, and also its security policies.

LogicGate had indicated to NYDIG that it has taken multiple steps in response to this incident. In addition to working with law enforcement and retaining Stroz Friedberg to assist in forensics and remediation, LogicGate deactivated and rotated credentials associated with its cloud computing platform and enhanced its authentication requirements. LogicGate also told NYDIG that it has activated additional information security monitoring and alerting, and conducted a targeted third-party audit of its cloud environment in addition to commencing a more comprehensive assessment of the environment to confirm its ongoing security. LogicGate has assured NYDIG that it is highly confident that the attacker no longer has access to its systems.

Although NYDIG's systems were not impacted by the attack on LogicGate, NYDIG is enhancing its security protocols around its systems to reduce the risks of any unauthorized use of NYDIG confidential data. In addition, NYDIG has raised awareness internally with its staff to be on heightened alert for any suspicious behavior that may be a direct result of the incident. NYDIG is also conducting dark web monitoring to determine whether the NYDIG data stored with LogicGate has been offered for sale by cyber criminals, and we have not seen any evidence of the data being exploited for any purpose.

NYDIG takes the protection of personal information of all of its stakeholders seriously and is committed to answering any questions that you may have. Please do not hesitate to contact me at the address above, at 1-212-909-6577, or agesser@debevoise.com.

Yours sincerely,

Avi Gesser

Avi Gesser
Partner

NYDIG

<<Client First Name>> <<Client Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Re: Notice of Data Breach

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

We are writing to notify you about a security incident that we have been made aware of at one of the vendors we utilize for onboarding new clients, LogicGate. Critically, there is no impact whatsoever to NYDIG's systems or to the assets held securely at NYDIG. However, we want to let you know about the incident promptly.

What Happened? LogicGate informed us on April 7th that an unauthorized third party accessed backups containing data of LogicGate's clients on February 23, 2021. Those backups include data from a system used by NYDIG for onboarding our clients and counterparties, as well as their authorized persons and related parties. NYDIG's data represented a small fraction of records in this vendor's systems, and we have not seen any evidence of NYDIG data stored within LogicGate being misused in any way. The incident potentially affected [X] [state] residents.

What Information was Involved? The impacted information includes: first and last names, dates of birth, social security or tax identification numbers, bank account numbers, passport and driver's license numbers, income, net worth, residential addresses, phone numbers, email address, and employment status.

What Are We Doing. NYDIG immediately activated its incident response procedures and has been in constant dialogue with the vendor to understand the nature of the breach and the potential impact to clients and counterparties. In addition to working with law enforcement, LogicGate has activated its internal data security response team and engaged outside forensics experts to conduct a review of the unauthorized activities. LogicGate is highly confident that the attacker no longer has access to its systems.

While, to date, we have no evidence of actual or attempted misuse of your information as a result of this incident, we are notifying you so that you may take further steps to better protect your personal information should you feel it is appropriate to do so. We also secured the services of NortonLifeLock, Inc. to provide identity and credit monitoring services at no cost to you for twenty-four (24) months. For more information on these services, please review the enclosed "Steps You Can Take to Protect Your Information."

What Can You Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity for the next twelve (12) to twenty-four (24) months. You may review the information contained in the attached "Steps You Can Take to Protect Your Information." You may also enroll in LifeLock Ultimate Plus to receive the identity and credit monitoring services we are making available to you as we are unable to enroll in these services on your behalf.

For More Information. While none of NYDIG's systems were impacted and your assets are safe, we take these matters extremely seriously and always seek to over-communicate. If you'd like to speak with us directly, we are here to help. You can contact NYDIG Client Services at (844) 511-0276 or clientservices@nydig.com for any questions related to the security incident. If you have additional questions regarding the LifeLock enrollment process, please call our call center at <<TOLL-FREE NUMBER>> (toll free), available 24/7.

Sincerely,

Kimberly Snuck
Client Services Manager

NYDIG

Steps You Can Take to Protect Your Information

Complimentary Credit Monitoring and Identity Protection Services

NYDIG has retained NortonLifeLock, Inc. to provide twenty-four (24) months of complimentary **LifeLock Ultimate Plus™** identity theft protection.

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to www.LifeLock.com. Click on the yellow "START MEMBERSHIP" button (do not attempt registration from a link presented by a search engine).
2. You will be taken to another page where, below the FOUR protection plan boxes, you may enter the **Promo Code: <<PROMO CODE>>** and click the "APPLY" button.
3. On the next screen, enter your **Member ID: <<MEMBER ID>>** and click the "APPLY" button.
4. Your complimentary offer is presented. Click the red "START YOUR MEMBERSHIP" button.
5. Once enrollment is completed, you will receive a confirmation email (be sure to follow ALL directions in this email).

Alternatively, to activate your membership over the phone, please call: <<TOLL-FREE NUMBER>>.

You will have until <<ENROLLMENT DEADLINE>> to enroll in this service.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your **LifeLock Ultimate Plus™** membership includes:

- ✔ LifeLock Identity Alert™ System†
- ✔ Dark Web Monitoring**
- ✔ LifeLock Privacy Monitor™
- ✔ USPS Address Change Verification
- ✔ Lost Wallet Protection
- ✔ Reduced Pre-Approved Credit Card Offers
- ✔ Fictitious Identity Monitoring
- ✔ Court Records Scanning
- ✔ Data Breach Notifications
- ✔ Credit, Checking and Savings Account Activity Alerts†**
- ✔ Checking and Savings Account Application Alerts†**
- ✔ Bank Account Takeover Alerts†**
- ✔ Investment Account Activity Alerts†**
- ✔ Three-Bureau Credit Monitoring[1]**
- ✔ Three-Bureau Annual Credit Reports and Credit Scores[1]**
  The credit scores provided are VantageScore 3.0 credit scores based on Equifax, Experian and TransUnion respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.
- ✔ File-Sharing Network Searches
- ✔ Sex Offender Registry Reports
- ✔ Priority 24/7 Live Member Support
- ✔ U.S.-Based Identity Restoration Specialists
- ✔ Stolen Funds Reimbursement up to $1 million†††
- ✔ Personal Expense Compensation up to $1 million†††
- ✔ Coverage for Lawyers and Experts up to $1 million†††

[1]If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the

verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.
No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.
**These features are not enabled upon enrollment. Member must take action to get their protection.
††† Reimbursement and Expense Compensation, each with limits of up to $1 million for Ultimate Plus. And up to $1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	**TransUnion** P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	**Equifax** P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services

In order 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 (5) 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	**TransUnion** P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	**Equifax** P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

NYDIG

Additional Information

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, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents: The Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or www.oag.state.md.us.

For Rhode Island residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; or 1-401-274-4400.

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 Maine, Maryland, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For Tennessee residents:

TENNESSEE CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE

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. A security freeze must be requested in writing by certified mail or by electronic means as provided by a consumer reporting agency. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. If you are actively seeking a new credit, loan, utility, or telephone account, you should understand that the procedures involved in lifting a security freeze may slow your applications for credit. You should plan ahead and lift a freeze in advance of actually applying for new credit. When you place a security freeze on your credit report, you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a period of time after the freeze is in place. To provide that authorization you must contact the consumer reporting agency and provide all of the following:

(1) The personal identification number or password;

(2) Proper identification to verify your identity; and

(3) The proper information regarding the period of time for which the report shall be available.

A consumer reporting agency must authorize the release of your credit report no later than fifteen (15) minutes after receiving the above information.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account, that requests information in your credit report for the purposes of fraud control, or reviewing or collecting the account. Reviewing the account includes activities related to account maintenance.

You should consider filing a complaint regarding your identity theft situation with the federal trade commission and the attorney general and reporter, either in writing or via their web sites.

You have a right to bring civil action against anyone, including a consumer reporting agency, which improperly obtains access to a file, misuses file data, or fails to correct inaccurate file data.

***