C/O IDX
10300 SW Greenburg Rd., Suite 570
Portland, OR 97223

If you ***haven't*** enrolled,
Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip Code>>

April 1, 2021

Re: Data Security Incident

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of an incident that may have involved your personal information. At Benetech Inc., we take the privacy and security of your information very seriously. We also want you to know that we took immediate steps to respond to the incident.

This letter contains information about the incident, as well as steps you can take to protect your information, including the resources we are making available to assist you in doing so.

What Happened: On March 2, 2021, we discovered suspicious activity. Right away, we investigated the activity, isolated the incident and secured the system. We quickly took measures to preserve personal data, including employee data, and began the forensic analysis of the incident, which was a rigorous process. We engaged two leading third-party computer forensic firms to conduct an independent investigation into what happened and whether any personal information may have been affected. We contacted federal investigators and have proceeded cautiously in order to coordinate our efforts with law enforcement.

The investigation recently determined that some of your personal information may have been affected as it was located on a drive that showed suspicious activity. At this time, we have no evidence to suggest that your personal information has been misused. Nonetheless, out of an abundance of caution, we are writing to inform you about the incident and to share with you steps you can take to protect your personal information.

What Information Was Involved: The following information may have been involved in the incident: your name, postal address, Social Security number, driver's license number, financial account information and/or drug screening information.

What We Are Doing: As soon as we discovered the incident, we took the steps described above. We also implemented additional security features for all of our endpoints to reduce the risk of a similar incident occurring in the future. We have been and continue to be committed to cyber hygiene and the implementation of industry-recognized standards and best business practices.

Though we are not aware of the misuse of any potentially impacted information, as we conveyed in our March 16, 2021, correspondence, we have made credit monitoring and identity protection services available to you at no cost through IDX (formerly known as ID Experts). These services include twelve months of Credit Monitoring, Dark Web Monitoring, $1 Million of reimbursement insurance, and unlimited access to the IDX member services team, who can address any questions or concerns you have.

To receive these services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. As we had explained on March 16, 2021, you **must enroll** in these services to receive them. We are extending the date by when you can enroll—until July 1, 2021, which is three months from the date of this letter. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: We encourage you to enroll in the services that we are offering you, and to follow the recommendations included with this letter. We also recommend that you review your credit report and consider placing a security freeze on your credit file. If you see anything that you do not understand or that looks suspicious, you should contact the three consumer reporting agencies listed under the section titled "Recommended Steps You Can Take to Further Protect Your Information" for assistance.

For More Information: Further information about how to protect your personal information appears on the following page.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, 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.

Please call 1-800-939-4170 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Thank you for your loyalty to Benetech and your patience through this incident. We take the privacy and security of your personal information seriously. We assure you that we took a deep look into this incident and appreciate your continued trust in us. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Mark Batchelor
Chief Financial Officer

Recommended Steps You Can Take to Further Protect Your Information

Enroll with IDX:

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect 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 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Review Your Credit Reports and Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant for the next twelve to twenty-four months and review your account statements and 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. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC"). You can request a copy of your credit report and rreport any fraudulent accounts to the credit reporting agency by visiting https://www.identitytheft.gov/.

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.

Copy of Credit Report: Under federal law, you are entitled, once every 12 months, to obtain a free copy of your credit report from each of the three major credit reporting agencies by visiting http://www.annualcreditreport.com/ or by calling toll-free 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.

To contact the three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

If you detect any information related to fraudulent transactions, you should notify the credit reporting agency that issued the report and have it deleted.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX 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.

Place Fraud Alerts: You may want to consider placing a fraud alert on your credit report 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. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. 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 identified above. **Please Note: No one is allowed to place a fraud alert on your credit report except you.**

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.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove a security freeze. There is no cost to freeze or unfreeze your credit files.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You are encouraged to report suspected identity theft to the FTC. You may also report suspected identity theft to local law enforcement, including the Attorney General in your state. Residents of North Carolina can obtain more information from their Attorney General using the contact information below.

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

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.

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

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.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.