16537

NOTICE OF DATA BREACH

All,

As a conscientious member of the technology industry, we take very seriously our responsibility to safeguard all sensitive and confidential information provided to us. For this reason, we are writing to inform you of an incident involving your personal information that occurred at Nextenture, Inc.

What Happened
We deeply regret that we are contacting you today to inform you of an incident that resulted in unauthorized access by an unknown individual or individuals to your personal information.

On February 24, 2020, a sophisticated hacker was able to "spoof" our CEO's email address meaning that the hacker was able to send an email to one of our employees that looked like it came from our CEO. The hacker's email asked for copies of employee W-2 forms. Notably, this hacker did not actually hack into our systems, and our systems were never compromised. But believing the email request to be legitimate, one of our employees sent W-2 forms, including yours, to this unknown individual or individuals on February 24, 2020. Upon discovery of the incident, we immediately notified the IRS. We will be notifying all state tax authorities where our employees file taxes in the next two days.

What Information Was Involved
The employee W-2 forms included your name, postal address, social security number marital status, employer information, salary details, employee benefit information, and certain tax return data, such as withholding information, exemptions and allowances.

What We Are Doing To Protect You
We are taking measures to minimize future risks to your privacy by reviewing and following our internal controls, notifying law enforcement, and providing you a full package of credit protection services, for two years, free-of-charge through **AllClearID**. More information on **AllClearID** will come out soon.

What You Can Do To Protect Yourself
We encourage you to remain vigilant by reviewing account statements and monitoring free credit reports. Access https://identitytheft.gov, click on "Get Started" button and follow the steps.

Tax-Related Identity Theft
The IRS is warning taxpayers of tax-related identity theft, which is an incident where someone uses your stolen Social Security Number and other tax information to file a tax return claiming a fraudulent refund. If you e-file your tax return and discover that a return has already been filed using your Social Security Number, or if the IRS sends you a letter reading that has identified a suspicious return using your Social Security Number, you should visit the IRS's identity theft web page at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft and follow the IRS's instructions. You can also visit that website in advance of any e-filing of your returns to explore identity theft protections offered by the IRS.

For More Information
The three major credit card reporting agencies can provide information and assist you should you wish to have a "fraud alert" or "security freeze" placed on your credit file. The following table provides contact information for these organizations.

Company	Website	Telephone	Mail
Equifax	www.equifax.com	1-800-525-6285	PO Box 740241, Atlanta GA 30374-0241
Experian	www.experian.com	1-888-397-3742	PO Box 2104, Allen, TX 75013-0949
Trans Union	www.transunion.com	1-800-680-7289	PO Box 1000, Chester, PA 19022

The Federal Trade Commission (FTC) also can provide information about identity theft, fraud alerts, and security freezes. The FTS may be contacted through its website (http://www.ftc.gov/), by calling its toll-free telephone number (1-877-438-4338), or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

More communication will follow.

Warm Regards,
Nikhil Kinikar | CEO | 339.364.0844