



February 24, 2023

Via email only to: ldtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Notice of Data Breach

Dear Sir/Madam:

High companies (High) is providing to the Maryland OAG notice of a printing error event which resulted in full Social Security Numbers (SSN) being printed on two (2) Maryland residents' 1099s. On January 30, 2023, High mailed the 1099s to the recipients in envelopes with cellophane windows and the full SSN may have been apparent through the window. On February 2, 2023, High learned of the printing error and to date, High does not have any information indicating that the SSNs were obtained and/or misused by unauthorized persons. High has since taken corrective measures to ensure the printing error does not occur in the future.

Although High does not believe that Maryland's data breach statute and its requirements are triggered because there was no breach of a security or computer system, nor was computerized data involved, High is providing information to the Maryland OAG in an abundance of caution. Enclosed is a copy of the letter High is sending to those Maryland residents whose full SSNs may have been apparent through the envelope window. The letter includes, among other things, a description of the events, when the 1099s were mailed, High's response, resources for the individuals who may have been impacted, and a 1-year identity theft and monitoring service that High is offering through NortonLifeLock at High's expense.

Should this notice be provided to any other unit of the Maryland OAG, please forward that information to High as soon as possible. Please contact me should you have any questions or require additional information.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'CH'.

Caroline Henrich,
General Counsel

Encl.



February 24, 2023

Recipient
Street Address
City, State Zip

RE: NOTICE OF DATA BREACH

Dear **Name**,

We are contacting you about a data breach that has occurred at the High companies (High).

What Happened and What Information Was Involved?

Consistent with our obligations to provide 1099s in advance of IRS payment reporting deadlines, on January 30, 2023, High mailed 1099s to certain individuals (Payees), via United States first class mail. On February 2, 2023, High learned that a subset of the 1099s inadvertently contained the Payees' full Social Security Number (SSN) and that the SSN may have been viewable through the envelope's cellophane address window. If you are receiving this letter, you are one of the Payees whose SSN was printed in-full on the 1099. To date, High does not have any information indicating that the SSNs were obtained and/or misused by unauthorized persons, however High is informing you of the issue and providing security measures to Payees as further outlined below.

High's Response

In response to these events, High is taking corrective action to remedy the processes that led to printing the full SSNs on the 1099s and to prevent 1099s from including full SSNs in the future. To protect Payees, High has retained NortonLifeLock to provide 1 year of complimentary **LifeLock Defender™ Preferred** identity theft protection. LifeLock provides credit monitoring and identity theft restoration services. A description of the **LifeLock Defender™ Preferred** service, along with steps to sign-up is enclosed.

The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111

Experian: experian.com/help or 1-888-397-3742

TransUnion: transunion.com/credit-help or 1-888-909-8872

February 24, 2023

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at [IdentityTheft.gov](https://www.identitytheft.gov) to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the website addresses or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it. It is advisable to remain vigilant by reviewing account statements.

We have also enclosed information from the FTC's website (which can also be accessed here: <https://www.identitytheft.gov/#/Info-Lost-or-Stolen>) about steps you can take to help protect yourself from identify theft.

For More Information

Payees can contact Kristine Cowfer at (717) 874-6446, or by email at High1099@high.net.

Very truly yours,



Karen A, Biondolillo,
SVP, Chief Financial Officer

Encl.