ComplyRight Data Security Incident Notice

ComplyRight was the victim of a criminal cyberattack. In late May 2018, ComplyRight was alerted to a potential issue affecting the tax form preparation websites using our platform. Upon learning of the potential issue, we disabled the platform and remediated the issue on the website. In consultation with third-party forensic cybersecurity experts, we took swift action to secure the data of our partners, business customers and the individuals potentially impacted.

The forensic investigators concluded that there was unauthorized access to our website resulting in compromise of personal information for some individual recipients of tax forms such as 1099 or W-2 forms. Although the forensic investigation determined the information was accessed and/or viewed, the investigators were unable to confirm whether the information was downloaded o otherwise acquired by the unauthorized user. And at this time, we are not aware of any reports of identity fraud as a direct result o this incident.

Nevertheless, out of an abundance of caution, we initiated a thorough communication plan to advise all affected businesses and individuals to explain what happened and provide the individuals with information (What to Do When You Receive a Data Breach Notice) and services to help safeguard them against identity fraud, including 12 months of free credit monitoring and identity theft protection services.

At ComplyRight, we take privacy and security very seriously and sincerely apologize for this occurrence. We have been providing businesses with tax reporting products and services for more than 30 years. We share your concern about cyber security and remain committed to continuously updating our practices to protect individual privacy.

ComplyRight Cyber Incident Update – July 18, 2018

We recognize how concerning this has been for those affected – and we are working diligently, within our company and with the support of outside experts, to answer your concerns and questions.

What happened?

On May 22, 2018, ComplyRight initially learned of a potential issue involving our tax reporting web platform. After investigation, we concluded that a criminal cyberattack had targeted some of the personal information maintained on the websites using our platform.

How did this happen?

The investigation determined there was unauthorized access to the ComplyRight web platform that is used by various websites to prepare tax-related forms for individuals (for example, 1099 and W-2 forms). Upon learning of the issue, we disabled the platform, remediated the issue on the website, and commenced a prompt and thorough investigation using external cybersecurity professionals to determine who was potentially affected and what information was accessed or viewed. Although the investigation determined the information was accessed and/or viewed, it could not confirm if the information was downloaded or otherwise acquired by an unauthorized user.

Who is affected?

A portion (less than 10%) of individuals with tax forms prepared on the ComplyRight web platform were impacted by this incident. All affected individuals have been sent notifications via U.S. Mail to their last known addresses. This letter included information to help safeguard them against identity fraud, including 12 months of free credit monitoring and identity theft protection services through TransUnion.

What information was involved?

The investigation confirmed that the portion of the website that was accessed contained names, addresses, phone numbers, email addresses, and Social Security numbers of individual tax form recipients.

Why did I receive a letter from ComplyRight?

ComplyRight provides a web platform used by a number of different tax form preparation websites. On behalf of those organizations and our clients, we executed the communication plan to advise those affected as promptly as possible.

This is not a scam, and we apologize for any confusion that may have arisen due to your lack of familiarity with our company.

Why did ComplyRight have my information?

Tax reporting forms (such as 1099s or W-2s) sent to you were prepared on a site using the ComplyRight web platform.

How am I affected if I am a site user or employer (payer)?

The investigation found no evidence that any user or payer information was compromised. No credit card or bank account information of users or payers was involved.

What has the unauthorized person(s) done with the individual information?

To date, we are not aware of any reports of identity fraud using individual tax form recipient information as a direct result of this incident. Although the investigation determined that the information was accessed and/or viewed on the website, it was unable to determine whether the information was downloaded or otherwise acquired. Nevertheless, out of an abundance of caution, we provided notice to all impacted individual tax form recipients. Further, we have no evidence that user or payer information was involved.

Did you report this incident to the appropriate authorities?

Yes. We have notified law enforcement of this incident. In addition, we have completed notification to the IRS and regulators, including state Offices of Attorney General, as required.

What else is ComplyRight doing in light of this incident?

ComplyRight has been providing businesses with tax reporting products and services for more than 30 years. We consistently endeavor to follow the best practices in data security and privacy, utilizing both internal and outside experts. This incident is unprecedented in our history and we immediately executed additional security measures and analysis of our platform and practices.

We remain committed to maintaining the privacy of information entrusted to us and, moving forward, we will continue to strengthen our security protocols and practices.

I have additional questions about my individual situation. What should I do?

Please call the number provided on your notification letter for immediate assistance.

Again, we extend our sincere apologies to those businesses and individuals affected by this incident. We understand your concern and will provide additional updates here, if applicable.