

December 2, 2020

Dear Tyler team members,

By now you have received many communications about Tyler's September 23 security incident involving ransomware and its impact on Tyler's internal systems. As part of our recovery process, we put all Tyler team members through a forced reset of passwords used with their Tyler email address and to access the Tyler network. We also advised you to change your password for any other account where you might use your Tyler username/password. We expect you have completed those steps by now.

Action Required: If you have not already done so, you should also change the password you use for all other websites or accounts that you visit using your Tyler device ***where you have (a) stored the password on your machine or (b) asked for it to be remembered in the browser you use to access the website or the account.*** We are making this recommendation Tyler-wide out of an abundance of caution.

Going forward, please follow these guidelines relating to username/passwords:

- Do not ask websites or accounts that you visit using your Tyler device to remember your password(s). Tyler has invested in a tool known as LastPass, a password manager that stores encrypted passwords online. We encourage you to take advantage of this tool. See [insideTyler for links to training and FAQs](#). You should have received an email invitation to create your LastPass account in April 2020. If you cannot locate the email, please contact the Help Desk.
- Do not use your work email address/password combination for any accounts that are not work-related, and do not use your work password for other accounts.
- Do not re-use the same password for more than one website or account. Visit the FTC's website for tips and tricks for creating a strong password: [h**ps://www.consumer.ftc.gov/blog/2015/07/advanced-password-tips-and-tricks](https://www.consumer.ftc.gov/blog/2015/07/advanced-password-tips-and-tricks).
- It is always a good idea to monitor your account statements and credit reports as part of your efforts against identity theft. You are entitled to a free credit report every year by law. During the coronavirus pandemic, those reports have been freely available on a weekly basis. You can visit the FTC website for more information: [h**ps://www.consumer.ftc.gov/articles/0155-free-credit-reports](https://www.consumer.ftc.gov/articles/0155-free-credit-reports). You can also receive information from the FTC about fraud alerts or security freezes. That information is also available from the three major credit bureaus. I have provided their contact information for your records at the bottom of this letter.

If you have any questions or concerns about these instructions, please email security@tylertech.com or call 1-888-558-9537.

Even as we resume more normalized operations, several groups are coordinating a "lessons learned" initiative, so you should expect to see and hear about new refinements as we apply

those lessons. We are investing in additional security enhancements, beyond those already part of our portfolio. Examples include:

- Maintaining supplemental threat detection software on all Tyler servers and workstations;
- Expanding the use of Okta multi-factor authentication across additional Tyler applications and tools; and
- Implementing further employee training on recognizing and responding to cyber threats.

It is important to remember that all internal communication related to this incident is privileged and confidential, and **should not be shared or discussed with clients**, family members, or any other individuals. We are providing approved information directly to clients at the appropriate time.

Thank you for your continued attention to these important requests and guidelines. And thank you again for the dedication and patience you brought to the incident response and recovery process. While this was a challenging time for all of us, your support and attention was a valuable part of our recovery process.

Thank you again,



Jeremy Ward

Vice President, Information Security

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
alerts.equifax.com

Experian Fraud Reporting 1-
888-397-3742
P.O. Box 9554
Allen, TX 75013
experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
transunion.com