Dear PCT member or supporter,

We are contacting you with the unfortunate news about a data breach that may have occurred with Pickerington Community Theatre (PCT). On January 31, 2017, we were the victim of a robbery. Among the things that were stolen was a large deposit from the last show and other miscellaneous checks. The deposit included cash and checks. A police report was filed immediately.

Because checks were stolen, anyone who has written a check to PCT in the last few months may be exposed to bank account theft. We are asking that you please monitor your bank account closely over the next several weeks. Although, we believe the criminals were trying to get cash and items they could sell, we have been advised that you may want to consider contacting your bank and speaking with them about the risks and precautions you can take to have checks temporarily held and place a fraud alert on your account. Your bank will also be able to advise you about the possibility of the need to close/change your bank account.

It is important to note, no credit card information was compromised. Also, no personal data, other than that listed on the checks, was compromised.

We sincerely apologize for any inconvenience this may cause. Please be assured PCT has developed a proactive plan and will take precautions to prevent anything like this from occurring again. The members of the community are our always first priority!

Please feel free to contact Jodi Weibel at (614) 562-4106 or [info@PCTshows.com](mailto:info@PCTshows.com) to discuss this matter in more depth. If you have friends or family who may be affected by this, please feel free to pass this letter on.

Thank you very much for your ongoing support.

Sincerely,

Andrew Weibel – President

Adam Schroeder – Vice President

Elaine Schroeder – Secretary

Jodi Weibel – Treasurer

Please see the attached for additional information about Identity Theft.

**Additional Information:**

Again, although we do not anticipate a personal identity theft problem, as no social security numbers were on the checks, it is still advisable to monitor your credit file and consider placing a fraud alert.

A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call 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 90 days.  You can renew it after 90 days.

Equifax: [equifax.com](http://www.equifax.com/) or [1-800-525-6285](tel:(800)%20525-6285)

Experian: [experian.com](http://www.experian.com/) or [1-888-397-3742](tel:(888)%20397-3742)

TransUnion: [transunion.com](http://www.transunion.com/) or [1-800-680-7289](tel:(800)%20680-7289)

Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report and call [insert contact information for law enforcement if authorized to do so]. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC’s site at [IdentityTheft.gov](http://www.identitytheft.gov/) to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC’s Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a credit freeze on your credit file.  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.  The cost to place and lift a freeze depends on state law.  Find your state Attorney General’s office at [naag.org](http://www.naag.org/) to learn more.

Please visit this link, [Identity Theft: A Recovery Guide](https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf), a comprehensive guide from the FTC to help you guard against and deal with identity theft or visit [identitytheft.gov](https://identitytheft.gov/%20%20) to learn about steps you can take to help protect yourself from identity theft, depending on the type of information exposed.