On May 9th, 2019 Aging, Disability & Transit Services of Rockingham County (ADTS) experienced a disruption in their internal Information Technology systems. Although it initially appeared that the incident was isolated to a small number of computers and the email system, it was later confirmed that the organization's server had been infected with ransomware, a specific type of malware that encrypts files on a system.

Although we are unaware of any acquisition or misuse of information related to this incident, regulations were recently tightened to reclassify this type of attack as a HIPPA 'breach.' As such, this incident requires notices and disclosures to those who could be affected.

The information at risk as a result of this incident includes names, addresses, contact details, social security numbers, dates of birth, health insurance numbers, medical diagnoses and treatment details.

We are now working with TruShield, a team of experts that deal specifically with cyber threats and attacks. The incident is being thoroughly investigated and we have taken immediate action to reinforce existing security measures, and rebuild with enhanced protections in place to mitigate any future risks.

A security breach happens when data or records containing personal information, such as Social Security numbers, credit card or bank account numbers or driver's license numbers are lost, stolen or accessed improperly. This kind of information can be used by criminals to commit identity theft.

What is a Security Breach?

A security breach happens when data or records containing personal information, such as Social Security numbers, credit card or bank account numbers or driver's license numbers are lost, stolen or accessed improperly. This kind of information can be used by criminals to commit identity theft.

Being notified that your information was part of a security breach does not necessarily mean you'll become a victim of identity theft. However, you are at a greater risk and need to take steps to protect yourself.

The NC Attorney General recommends taking the following steps to protect your information:

Step 1: Check affected accounts
If the security breach involved credit cards, debit cards or specific accounts, check your statements for those accounts immediately.

If you see any activity that you did not authorize, contact the bank or company that services the account immediately to report the fraud. You should also request a new credit or debit card with a different number and change any PINs or passwords for the account.

Step 2: Sign Up for Free Services
Some businesses or government agencies offer security breach victims a free service such as credit monitoring. While most offers are genuine, don't provide private information without verifying that the credit monitoring service is legitimate.

Step 3: Notify the Credit Bureaus
Request a fraud alert from one of the credit bureaus. This tells banks and other creditors to take extra steps to verify your identity before issuing credit in your name. A fraud alert is free and will last 90 days unless you request an extended seven-year fraud alert and provide a police report

You'll also get a free copy of your credit report, which you should review carefully.

To request a fraud alert, contact one of the three nationwide credit bureaus.

Equifax 1-800-525-6285
Experian 1-888-397-3742
TransUnion 1-800-680-7289

Step 4: Consider a Security Freeze
A security freeze stops access to new credit in your name. Placing a security freeze prohibits credit reporting agencies from releasing any information about you to new creditors without your approval, making it difficult for an identity thief to use your information to open an account or obtain credit.

North Carolina consumers can now get free security freezes online. Identity theft victims who have filed a police report, their spouses, and consumers over the age of 62 can also get free security freezes by mail or phone. Other consumers can get security freezes by mail or phone for a fee.

Under a new North Carolina law, parents and guardians can shield their children's credit report with a special Protected Consumer security freeze. This law can also be used to protect the credit reports of incapacitated adults.

Step 5: Monitor Your Credit
Continue to review your credit reports every few months. Your private information that was released in the security breach may not be used right away. You can request a free credit report annually.

Notifying Law Enforcement
Most law enforcement will not issue you a police report until your private information is actually used by an ID thief. If you have any suspicion that your information is being used by a thief, contact local law enforcement immediately.

Aging, Disability and Transit Services has established a dedicated assistance line for individuals seeking additional information regarding this incident. If you have questions or concerns, please contact 1-800-674-6920.