EQUIFAX DATA BREACH – IS YOUR IDENTITY AT RISK?

With over 143 million records compromised, it is very likely that your personal data was compromised in the Equifax data breach. This is particularly troubling because this was a breach of one of the companies that is supposed to be providing credit and identify protection services. Social security numbers, birth dates, addresses, and driver's license numbers might have been accessed. This is the information someone could use to open bank accounts, credit cards, and loans in your name, as well as file fraudulent tax returns.

Please know that this was NOT a breach of Iroquois Federal's data systems. We are sharing this information about Equifax to ensure that you are aware of the issue and take the proper precautions to reduce your chances of becoming a victim of identify theft and fraud.

First and foremost, find out whether your information was compromised. Equifax has established a special website to provide updated information to consumers:
Go to www.equifaxsecurity2017.com and select "Potential Impact" to see whether your data was involved. The irony is that they will ask for the last 6 digits of your social security number along with your last name. Be sure that you are using a secure connection (e.g., not public wireless network) when entering this information.

Steps to take if your information was compromised:

- **Enroll in TrustedID Premier.** You can enroll directly from the Equifax web site. It provides you with copies of your Equifax credit report, the ability to lock your Equifax credit report, credit monitoring of your Equifax, Experian, and TransUnion credit reports Internet scanning for your social security number and identity theft insurance. Contrary to earlier reports, the Equifax website states that by opting in to this service you are *not* waiving your legal rights for this cyber incident.
- **Check your credit reports.** You can do this by visiting www.annualcreditreport.com or through TrustedID Premier.
- **Place a fraud alert on your records.** A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name is really you. Once you place a fraud alert with one nationwide consumer reporting agency, it will be automatically placed with the other two nationwide consumer reporting agencies.
- **Consider placing a credit freeze with Equifax, Experian, and Transunion.** This is in lieu of placing a fraud alert and provides additional protection. A credit freeze makes it even more difficult for a fraudster to open accounts in your name. It is a good idea to place a credit freeze on your children—if allowed by your state—if they are not going to be applying for any credit accounts in the near term. Click here for more information about putting a credit freeze on your child's account.
- **Consider buying additional fraud protection.** Companies like LifeLock, EZShield, and Identity Guard provide enhanced monitoring and remediation services for a fee.
- **Monitor your bank and credit card accounts closely.** Keep an eye open for fraudulent activity and report it immediately.

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement. The Federal Trade Commission provides useful tools to assist you in the event your identity has been compromised. For more information, see their Identity Theft Consumer Information.

Please contact Equifax with specific questions about the breach and how it effects your information. They have set up a **dedicated call center at 866-447-7559.** If you have other questions, feel free to contact us.