Identity Theft & Fraud Prevention (rev. 2.1.21)

1. **Never provide personal financial information**, including your Social Security number, account numbers or passwords, over the phone or the internet if you did not initiate the communication. If you believe the contact may be legitimate, contact the organization yourself using a phone number or website address that you have independently obtained.
2. **Do not be intimidated** by an email or caller who suggests dire consequences if you do not immediately provide or verify financial information.
3. **Do not be enticed** by offers that seem too good to be true. These offers are often used to get you to drop your guard and share personal financial information.
4. **Never click on the link provided in an unsolicited email.** It may contain a virus that can contaminate your computer, or software code that will capture your passwords when you log on to websites.
5. **Change your password periodically** and use different passwords for different websites.
6. **Routinely monitor** your financial accounts and billing statements.
7. **Shred documents** containing personal financial information.
8. **Visit www.ftc.gov/bcp/edu/microsites/idtheft/**, or call 1-877-IDTHEFT for additional advice.

<u>If you believe you have disclosed personal financial information to a thief, take the following actions.</u>

1. Contact Michigan One and your other financial institutions. Close accounts that you know or believe may be at risk.

2. Contact one of the three major credit bureaus to place a fraud alert on your file to prevent thieves from opening new credit in your name.

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

3. Report suspicious emails or calls to the Federal Trade Commission via the internet at www.consumer.gov/idtheft , or by calling 1-877-IDTHEFT.

4. File a report with your local police or the police in the community where the identity theft took place.