Anti-Fraud Tips:

- Set up MemberDirect “Alerts” in Online Banking to be notified of suspicious activity.

- Keep your computer’s anti-virus and anti-malware software up to date.

- Avoid using online banking via free public wifi such as those at coffee shops and hotels.

- Always use strong passwords containing capital letters, numbers, and special characters.

- Protect your PIN for your debit/credit cards and avoid sharing it with others. Never write your PIN on your cards.

- “Phishing” was one of the leading causes of fraud last year. This is when hackers send emails, texts, or phone calls impersonating a reputable business. Common Phishing scams include emails/popups/texts claiming to be from MicroSoft, Interac, delivery companies (UPS/FedEx/Canada Post), CRA, your Telephone provider, your bank/credit union, or other reputable businesses. Unfortunately, you can’t trust anyone who calls or emails today. If in doubt, hang up and call the company on a trusted number.

- Monitor your credit card and other accounts for suspicious activity. Though fraud detection systems are advanced, keeping an eye on your accounts for suspicious transactions is good practice.

- Check your credit report occasionally to ensure someone isn’t using your identity. If you’re speaking to one of our lenders, they can review it with you. Or, you can request a copy from Equifax or Transunion for free via phone or mail.

- When paying online, be sure you are on a reputable, trusted website and on a secure network (Not free public wifi).

- If you are not expecting an e-transfer, do not click on an e-transfer email.

- For an in-depth list of common scams, visit the “Canadian Anti-Fraud Centre” online.