SIM Swap Fraud

SIM SWAP FRAUD IS A TYPE OF ACCOUNT TAKEOVER FRAUD.

A criminal's objective in the SIM swap fraud is to gain control of your mobile services by linking it to a new SIM card, which is in a device that they have control over. This type of scam includes:

- **An individual being the subject of SMShing campaign where the individual is directed to spoofed websites and credentials are harvested.**
- **In addition to credentials, members have been asked to input DOB, SIN, and answers to security questions etc.**
- **Through the SMShing attack, the hacker uses the harvested information to socially engineer the member's telecommunications company and have the member's number ported to a new phone and SIM card.**
- **Hacker then quickly completes fraudulent transfers.**
- **When credit unions called the members (from information they had on file), the staff were advised by the person on the other end that these transactions were legitimate.**
- **In fact, these transactions were not legitimate, as staff were talking directly to the hackers.**

PROTECT YOURSELF & THE BUSINESS FROM THIS SCAM:

- **Avoid publishing personal information on social media (e.g. date of birth, telephone number, postal code, spouse's name etc.).**
- **Advise members that your credit union will never contact them in an unsolicited manner and ask for personally identifiable information (PII).**
- **Members should be encouraged to increase the security around their telecommunications account.**

VP Credit Union
SINCE 1944