ARBOR
FINANCIAL CREDIT UNION

Compromised Account - What's Next?

Important Steps to Take if Your **BANK ACCOUNT** has Been Compromised

If your bank account has been compromised, then it is recommended that you ***complete the following in two weeks,*** after which time your compromised account will be closed.

- ☐ **Set new passwords and PINs:** this is also a good time to choose new security questions and update your contact information online.
- ☐ **Change your direct deposits:** After you establish a new bank account, be sure to update your direct deposits, so they link to your new account, by contacting either your employer's human resource department or the Social Security office at www.ssa.gov
- ☐ **Update your automatic payments:** If your bills are automatically deducted from your bank account, credit card, or debit card, then you will want to update the payment information with your new bank account information.
- ☐ **Contact anyone that has an uncashed check:** they will need to cash the check within two weeks otherwise a new check will need to be written.

Important Steps to Take if Your **PERSONAL INFORMATION** has Been Compromised

- ☐ **Report identity theft and get a recovery plan at IdentityTheft.gov:** This is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.
- ☐ **Log-in or Sign up for IDProtect:** You'll want to make sure your contact information is up to date, and credit alerts are set up. You can also review your credit report and have an agent assigned to your case to help you through the identity theft process. If you need assistance signing-in, please contact us.
- ☐ **Place a fraud alert:** You can place a free, one-year fraud alert by contacting one of the three credit bureaus below. That bureau must inform the other two.
  - ☐ Equifax: 888-378-4329
  - ☐ Experian: 888-397-3742
  - ☐ TransUnion: 800-916-8800
- ☐ **File a police report:** If funds were stolen you will want to file a report with the police in the county where the loss occurred.

** For tips on preventing fraud see reverse side.*

ARBOR
FINANCIAL CREDIT UNION

Tips to Avoid Fraud

Here are some simple steps you can take to reduce or minimize the risk of becoming a victim of identity theft and fraud.

- If your computer is compromised, disconnect it from Wi-fi, unplug it, and power it down. The goal is to prevent the virus from spreading. Its recommended you bring it to a computer repair center for diagnosis.
- Don't give your personal or banking information out over the phone or via email. Arbor Financial will never ask you this information over the phone.
- Use caution and ask questions with any checks received in the mail that you were not expecting.
- Don't send funds to anyone you do not know personally.
- Don't enter sensitive information, like passwords, when connected to public Wi-fi.
- Never click on links from unsolicited emails or texts as they may contain a virus which could enable a hacker access to your data.
- Never send funds to anyone you do not personally know.
- Do not place checks in your personal mailbox for pick up by the postal worker.
- Call Arbor Financial at 269.375.6702 to report stolen checks.
- Shred old checks before throwing them away.
- Visit our security center for more tips: www.arborfcu.org/security-center