PERSONAL INFORMATION AND SECURITY

iQcu invests a great deal to ensure our computer systems, networks and access points are secure. Protecting your confidential account information is one of our highest priorities. It is equally important for you to take the necessary steps to make sure your confidential account and personal information is not compromised due to vulnerabilities in your computer systems or behaviors.

Your personal information

iQcu has policies and procedures in place to safeguard your personal information, whether it is obtained online, in person, or on paper. Specifically, for all online transactions, we use industry-standard encryption technologies.

Protecting your accounts

iQ never communicates requests for sensitive information either through email or text messaging (such as Social Security numbers, Telephone Banking PINs, passwords, or account numbers). If you receive an email or text message requesting this type of information, please contact iQ immediately.

Protecting your accounts Information collected through the use of our sites

We protect your personal information by taking steps to keep it secure and confidential. We have not and will not sell your account information.

Our site makes use of a feature of your web browser called "cookies". A cookie is used to personalize your iQ website experience. We also collect aggregate information about the use of our site that does not personally identify you, unless you have previously logged in to the site using the same device. These cookies may be used to present advertisements about our products and services that may interest you. These advertisements may appear on the iQ site or other websites. Please review these services:

Security

You communicate with our computer, systems and websites, by using your computer's web browser. For an optimal experience and to ensure safe and secure use of our website, your web browser will need to be updated periodically. iQ recommends using the most up-to-date version of your web browser.

iQ provides secure financial services through a protocol known as the Secure Sockets Layer (SSL). SSL prevents other computers along the route from eavesdropping by encrypting all data transmitted between our site and your computer. The sending end encrypts or encodes the data with one key before it is transmitted. The receiving end decrypts or decodes the data with another key.

The Secure Sockets Layer ensures that the data transmitted between your computer and our site has not been tampered with. Our site requires you to use a browser that supports SSL and cookies.

Account and Card Fraud Monitoring and Detection

iQ employs leading technology in fraud monitoring and detection. These strategies play a critical role in enabling iQ to protect your assets by allowing us to identify threats before they become issues and take preventive measures to protect your accounts and cards from loss. Fraud prevention is a joint effort between the credit union and its membership. We ask that you notify your local branch or the Member Solutions Center if you plan to travel or will

have out-of-the-ordinary expenditures. In addition, please advise us of any changes to your home, mobile or office phone numbers to allow for quick contact.

California Online Privacy Protection Act

iQ does not disclose the user's information to anyone else, although we may use cookies or other technologies to track where users originate, which of our web pages they visit and to help us identify them.

Children’s online privacy

iQ complies with the U.S. Children's Online Privacy Protection Act (COPPA) which requires us to notify and obtain consent from a parent or guardian before we collect, use and disclose the personal information of children under 13 years of age. We do not knowingly collect personal information from children under 13 years of age without such consent and if we learn we have inadvertently done so, we will promptly delete it.

Current threats

Minimizing the risk of current threats is a cooperative effort between iQcu and our members. Be cautious and aware of the current threats that could affect you: malware, phishing, smishing and vishing!

iQcu will not ask for personal information such as online credentials, account numbers or card numbers through e-mail, voice or text messaging.

E-mail Fraud (Phishing): Phishing e-mails will often provide a website link that will direct you to a fake website. Don't be fooled! When you sign in to iQcu's Online Banking, the security image and phrase you chose will appear to verify that you are on our official site.

Malware: Malware includes all types of unwanted software such as computer viruses, worms, Trojan horses, spyware and adware that can create a pathway for criminals to gain personal information.

Text Messaging Fraud (Smishing): Smishing uses mobile phone text messages to trick you into divulging your personal information. Often these messages will give the appearance that immediate attention is needed.

Voice Messaging Fraud (Vishing): Vishing is facilitated by Voice Over Internet Phone (VoIP) to gain access to your private personal and financial information.

Changes

We reserve the right to change this statement, and you agree it is your responsibility to check this statement periodically for any changes.