creb®

What is MFA?

Multifactor authentication (MFA) is a more secure way of logging into systems, by utilizing your password along with a code sent to your phone or email.

Why is Pillar9™ implementing MFA now?

Cyber attacks have evolved to the point where passwords alone are not secure enough. MFA has now become a default requirement and is often enforced by cybersecurity insurance providers. MFA will help ensure that your account as well as the MLS® database is kept secure from fraud and attacks.

Will I be prompted for MFA every time I login?

No. There are certain things that will trigger MFA to be required on a login every time including:

- New accounts
- First time logging in on a new device
- Recent email, phone number or password change

In addition, certain factors are considered and may trigger an MFA challenge, such as:

- Logging in from a new geographic location
- Too frequent logins
- Possible account sharing detection

Once the update is live, you will be asked for MFA frequently at first while the program is learning. This should taper off quickly, though.

What will happen when I am challenged for MFA?

When you are challenged for MFA you will be prompted to receive a code through email or SMS. The code will be sent to the email address or phone number on file. Once you receive your code, type it into the prompt and you will be logged in.

If you choose to receive the code through email, the email will come from do-not-reply@corelogic.com or do-not-reply@cotality.com.

If MFA makes things more secure should it not be required on every login?

While requiring MFA on every login would be more secure, a balance must be struck between security and convenience. By using the Clareity Assure engine to analyze logins and selectively challenge MFA we believe there will be balance between convenience and security.

What do I need to do before MFA?

Before May 27, please check that your contact information is accurate at https://www.creblink.com/Profile/Personal_Information/. The Direct Phone and Email fields are what you need to check for accuracy as that is where the MFA codes will be sent when needed.

Are there any other ways to authenticate besides Email and SMS?

Biometric (Face-ID, Fingerprint) passkeys may be available on your devices. Instructions on how to set these up will be communicated shortly after launch.

What else do I need to know?

Logins will be unavailable on May 27, from 3 a.m. to 5 a.m.