# BCrypt FAQ

**Q: What is BCrypt and why is it important?**
A: BCrypt is a secure password hashing function that enhances the protection of user passwords by making them harder to crack. It uses SALT protocol to defend against rainbow table attacks and a work factor to slow down potential attackers.

**Q: What do I need to do as a consumer user?**
A: Simply log into your digital banking account before June 4, 2025. This action will encrypt your password with the new BCrypt hashing algorithm. If you do not log in by the deadline, you will be locked out and will need to reset your password.

**Q: If I have logged in using my username and password since January 1, do I have to do anything?**
A: No, your password has been updated using the new BCrypt hashing algorithm and you do not need to do anything. You may continue to access digital banking as normal.

**Q: Do I have to log in to the browser and the mobile application separately to satisfy the login requirements?**
A: No, a log in on either the browser or the mobile application with your username and password will initiate the password rehash.

**Q: What do I have to do if I use biometrics to log in to my mobile application?**
A: If you only logged in using your biometrics during this period before June 4, 2025, you will need to log in using your username and password so the rehash can happen. If you are locked out and you reset your password, you will need to reenable your biometrics on the mobile application. However, you do not need to set up new biometrics on the device. Note: Biometrics information is only stored on the device, not with the digital banking applications.

**Q: What is the process of logging in for biometrics users?**
A: If you log in after June 4, 2025 using your biometrics, you can continue to log in until such time your biometrics fail or you are prompted to log in using their username and password. If you log in after June 4, 2025 using your username and password, it will fail, and you will need to do a password reset before you can reenable your biometrics again.

**Q: What should business users do if they get locked out?**
A: If you are a business user who gets locked out after June 4, 2025, you will need your Business Administrator to reset your password. Business Administrators can do this by logging into banking and using the Manage Users functionality to reset the password.

**Q: If a customer signs into the OLB on their regular computer (and the rehash occurs) and then they sign in via their mobile device with bio-metrics will this issue be resolved with the initial rehash or is the rehash also needed in their mobile device (that uses the bio metrics to sign in)?**
A: They will have their password rehashed during their log in to the computer. They will need to enable

their biometrics when they sign in to their mobile device to associate their biometrics to the new rehashed password.

**Q: How will this change improve security?**
A: Migrating to BCrypt for password hashing adds an additional layer of security by making it more difficult for attackers to crack passwords. This aligns with OWASP Application Security Verification Standard (ASVS) recommendations and helps protect user data.

**Q: What if I need help during the transition?**
A: Our digital banking support team is available to assist you during this transition. Please reach out to us at (618) 344-3172 or at depositservices@collinsvillebuildingandloan.com for any help regarding the migration or password reset process.