FORUM® CREDIT UNION

Application: **Business Online Banking**
Subject: **RSA Multifactor Authentication**
Date: **July 2018**

Overview

This document is provided to help expose and educate current and new Business Online Banking users implementing RSA Multifactor Authentication.

RSA Multifactor Authentication

When you log in to Business Online Banking beginning in July, you will begin a new RSA Multifactor Authentication process. RSA Multifactor Authentication starts off in the "silent period". This begins when you log in to Business Online Banking. During this time period, RSA multifactor authentication is gathering standard information about your online access. This includes information when you log on, such as time frames, IP addresses, etc.

This allows RSA multifactor authentication to build a profile of you that the system will use to check and make sure that you are in fact who you are signing on as.

Phase two is the "collection period". The collection period is broken down into four week long periods, and during each period, a randomly selected subset of all business online banking users is selected to answer five challenge questions.

The collection period is as follows:

Week 1 – 20%
Week 2 – 40%
Week 3 – 70%
Week 4 – 100%

Once the collection period has completed, you then enter the "Authentication Period".

During this period, when users log in to Business Online Banking, RSA multifactor authentication will check the sign in against a pattern of established behavior to establish a risk score. If the sign on is deemed to be an at risk attempt, the user will be prompted to answer two of their questions. Upon successfully answering their questions, they will be signed into Business Online Banking.

User Continually Gets Recollected

Occasionally, some users will be recollected. If a user continues to get recollected a FORUM employee may need to review RSA multifactor authentication and check phone settings.