

Navigating Security MFAs

Enhanced security features within the Rogue mobile app monitor and prompt multi-factor authentications (MFAs) when accessing high-security areas or displaying unusual banking behaviors. Follow these steps when navigating this added layer of protection.



When high-security areas are accessed or unusual banking behaviors are identified, you will receive a multi-factor authentication (MFA).



Choose your preferred method of delivery (text or call).



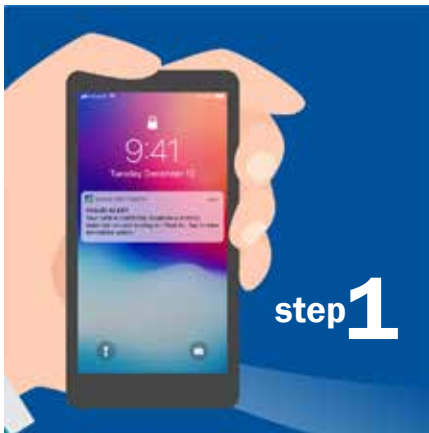
Complete your preferred method of authentication.



Once verified, you may continue with your banking activity.

Managing Real-Time Fraud Alerts

Receive real-time fraud alerts within the Rogue mobile app. Push notifications must be enabled to receive fraud alerts. Follow the steps below when you receive an alert.



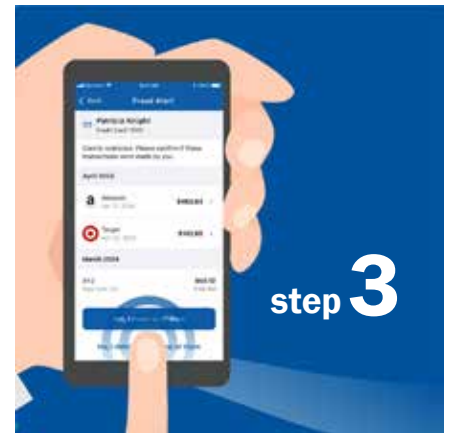
step **1**

Suspicious card transactions will trigger a real-time fraud alert to your device.



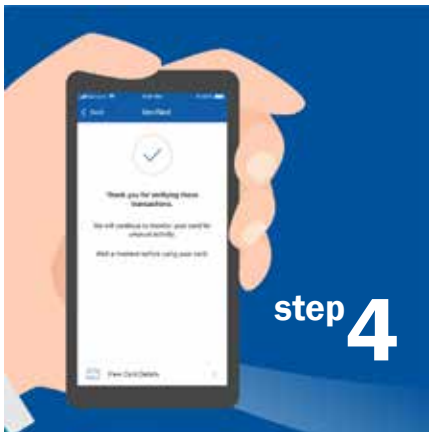
step **2**

Log-in to the mobile app to review transactions flagged as suspicious.



step **3**

If the transactions are legitimate, accept the transactions.



step **4**

The temporary card block is removed making your Rogue card ready for use.



step **5**

If one or more of the transactions are fraudulent, deny the transactions.



step **6**

A permanent block is applied to your card requiring a card replacement order by calling us at 800.856.7328.