Are your fraud protection efforts keeping pace as fraud evolves?

The fraud threat landscape continues to evolve, with attacks increasing in frequency and sophistication and becoming more difficult to prevent, resulting in billions of dollars in financial losses annually. Cybercriminals are using advanced techniques to steal data and siphon funds from businesses. By 2019, it is estimated the worldwide cost of cybercrime will top $2 trillion.[1] As cybercriminals get smarter and more adept at covering their tracks, it makes a multi-layered approach to security and fraud protection vital to safeguarding your company's assets and information.

Banks and other providers of secure, online services typically rely on multi-factored authentication to verify identity easily and protect data and transactions. A multi-layered approach is fundamental to keeping one's identity, data and transactions secure. Two-factor authentication was once thought to be a silver bullet to prevent fraud. According to Centrify, only a small percentage of cyber security professionals believe that user name and password-based security remains an adequate form of protection.[2] As a result, more companies are starting to use multi-factor authentication to reduce the risk of fraud and boost security.

What does a multi-layered authentication strategy look like? It combines knowledge, possession and inherence factors.[3]

- Knowledge factors include something only the user knows, such as a password, PIN or answers to secret questions.
- Possession factors leverage something only the user has, such as a smartphone, physical token, or a one-time password sent to the user's phone or email account.
- Inherence factors include something a user is, which would include all biometrics data such as fingerprints, voice prints and iris scans.
- For multi-factor authentication to be successful, it's important to strike a balance between convenience and security. A "one-size fits all" approach for authentication simply won't work. By offering a choice of authentication methods, individuals can choose which ones work best for their given situation.

Fortunately, there are a wide range of authentication methods available today, including:

- **Hardware tokens:** These are small hardware devices that a user carries to authorize access. They come in different forms, including token key fobs. The hardware device generates a code that the user enters when prompted.
- **Soft tokens:** These are software-based tokens or applications that generate a token code. They are typically mobile apps installed on a smartphone, and can take advantage of push notifications for improved user convenience. The widespread adoption of mobile devices has made soft tokens a popular option.
- **SMS/Text message:** A security code is sent to a phone via SMS. Once the user receives the text message, they enter the code into the login screen.
- **Phone call:** With this authentication method, a user receives a phone call to a registered phone number (landline or mobile number). The user then provides the correct response to the voice prompt to complete authentication. The advantage of a phone call (and SMS) is that the user is not required to own a smartphone.
- **Email:** A user receives an email with a link to verify the authentication request. Clicking on the link completes the authentication process.
- **Security questions:** Instead of tokens, users provide answers to security questions. These questions can be predefined or the user can define their own questions.
- **Biometric:** Methods include fingerprint, iris or retina scans, voice and facial recognition, and more. With smartphones being one of the three "must-have" items when leaving the home, along with house keys and wallet, smartphones will likely continue to increase in value as a critical part of a multi-layered authentication strategy.

As cyber threats continue to evolve, it's even more important than ever to take reasonable steps to secure and protect data and transactions. Using multi-layered authentication methods can help strengthen security-sensitive data and transactions as well as protect individual identity.

If you suspect fraud, contact your Wells Fargo representative, or call 1-888-937-9997, Monday through Friday, 5:00 a.m. to 7:00 p.m. Pacific Time, and ask to have a Wells Fargo Dealer Services Commercial Relationship Manager in your area contact you.

1. "20 Eye-Opening Cybercrime Statistics," by Bill Laberis, securityintelligence.com, November 14, 2016.

2. "Level Up Your Security: Best Practices for Multi-Factor Authentication," centrify.com, 2016.

3. "Muscling Up On Strong Authentication: Best Practices," second edition, entersekt.com, September 2016.