Using Biometrics While Mitigating The Risks

biometrics business customers digital banking

Summary: The global biometrics market is expected to hit $68.6B in 2025. While community financial institutions should be incorporating biometrics to protect customer data, they also need to mitigate the risks associated with biometrics. Data breaches, AI use to mimic behavioral biometrics, and security system workarounds are a few risks that need to be mitigated to stay safe as biometrics are integrated.

Biometrics use has been growing steadily and is expected to only speed up. The global biometrics market is expected to reach $68.6B in 2025, with a compound annual growth rate (CAGR) of 13.4%. It is important for community financial institutions (CFIs) to incorporate biometrics as they provide an important way to protect customer data. Still, there are risks. We give you an update on biometrics and how to mitigate the evolving risks.

Biometrics have come a long way. According to the Biometrics Institute, there are currently 15 different types of biometric data. Facial patterns, iris scanning, and hand geometry plus 11 others are added to the more everyday type of biometrics, fingerprints. While many financial institutions have embraced biometric tools, such as fingerprint scanning, as a way of combatting fraud, universal adoption is still not here yet.

Nonetheless, major advancements have already taken place and biometrics technology is now able to verify an individual's identity through more sophisticated factors, such as their behavior. These types of biometrics include an individual's posture, the way they use the computer, the places that they go online, their voice, the facial gestures that they make, and even how quickly they text.

Know the risks and how to mitigate them. Yet, protecting biometrics data is critical. Not only does it make good business sense to protect your assets and your reputation, but also examiners generally review these practices as part of your institution's Information Security Program (see FFIEC Information Security).

Data breaches. Since basic biometrics measures such as fingerprints and iris scans require storing scans as a basis for comparison, it creates the risk that if such data is breached it could be used to gain access to an individual's accounts. In addition to that, there have been cases where criminals have successfully spoofed fingerprints, bypassing such security measures.

To help **mitigate data breaches**, remember to:

1. **Prioritize data protection** – review your data and focus on sensitive data so that you don't dilute your security efforts which could jeopardize data unnecessarily
2. **Document your response process** – this is a given, but ensure it is reviewed regularly to be current with the latest cyber breaching methods
3. **Train and test** – make sure that you conduct drills to test your team for data breaches so that procedures and practices can be adjusted as needed before it could be more costly
4. **Be comprehensive** – if a data breach happens, make sure to research beyond the apparent attack details in case there was more underlying damage planted, bring in 3rd party experts when needed, and know

when and how to prepare and file a Suspicious Activities Report.

Behavioral monitoring risks. Though community financial institutions should not overlook the benefits of behavioral biometrics and the ways that they can bolster more basic biometric methods, they are not without their risks. In the same way that artificial intelligence can be used to identify an individual's unique characteristics and mannerisms, it **can also be used to mimic** these things. Behavioral biometrics also require constant monitoring of users to acquire enough data for a solid comparison basis. Failing to continuously update and maintain the system used to identify such characteristics could create additional risks, as hackers can **find ways around online security measures** quickly these days. Given this reality, CFIs that choose to go down this road should make sure they have the technical expertise necessary to keep such fraud measures timely and effective and to avoid the possibility that they could create unintended risks.

Regulatory references for mitigation. While there is evolving regulatory guidance on biometrics specifically, there are sources that bankers can reference to help with continuing mitigation. The FFIEC's Retail Payment System's booklet has a section on biometrics that provides direction on authentication and authorization. As this technology has developed, states have passed specific biometric privacy laws, including IL and TX. Others, such as CA, NY, and AR have incorporated biometrics into existing privacy laws. Check your state regulations to provide greater direction. Lastly, from a federal perspective, Gramm-Leach-Bliley Act (GLBA) gives broad guidance in protecting consumer personal information which, these days, would include biometrics.

Biometrics are an important way for CFIs to keep their customers' data safe. Yet, there are risks. Knowing them and mitigating them as they evolve are critical for your institution and your customers to stay safe.

SHARE THE BID WITH A COLLEAGUE

Would someone at your financial institution want to receive our complimentary BID publication? Share this BID via email.