Sell your biometric product.

Case 1: A bank needs an appropriate authentication mechanism to allow remote user transactions. What kind of multifactor system would you sell them?

Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system or within an authentication server.

MFA, also known as two-factor authentication or 2FA, is a security feature that allows you to log in to an account using two pieces of evidence - your credentials. Your credentials can be something you know (like a password or PIN), something you have (like a smart card), or something you are (like a smart card) (like your fingerprint). To be deemed multi-factor, your credentials must come from two separate categories. Entering two different passwords would not be considered multi-factor. MFA operates by requesting further information for verification (factors). OTPs are the four to eight-digit codes that you frequently receive via email, SMS, or a mobile app. When using OTPs, a fresh code is created on a regular basis or whenever an authentication request is made. The code is created using a seed value supplied to the user when they first register, as well as another component, such as an incremental counter or a time value.
We're working on a banking system that allows users to check in to the bank's website and confirm their identities when a transaction takes place. The reference data required for verification is stored and compared in the portal. Several authentication methods will be used throughout the procedure. The user can use their smartphone to access the bank's application.

Biometric authentication would be feasible in this case. Biometric authentication, which is simple to use, allows users to log in in seconds. Almost every smartphone nowadays has a fingerprint sensor.

Because most smartphones already have a fingerprint sensor, fingerprint recognition is accurate, simple to use, and cost effective among the most often used biometrics - fingerprint, palm veins,

face recognition, voice recognition, and iris scan. We can add password/pin authentication to the application's login procedure because biometrics aren't totally reliable.

The issues with phishing are clearly created by an overreliance on the first group, according to this perspective. Strong authentication could be achieved by using two different authentication credentials from different categories at the same time. Two-factor authentication is what it's called (2FA). Because of concerns regarding cost, complexity, reliability, and privacy, biometrics are not extensively employed in banking. However, there is a wide range of low-cost, reliable security devices available.

A One-Time Password is frequently generated and displayed by these security devices (or OTP). OTPs are only valid for one use and are often time-limited. In the sense that they can be generated on demand from an infinite sequence that is unique to each device, OTPs are dynamic rather than static. The consumer copies the OTP from the device to the web terminal. When combined with a traditional static password, knowledge of a valid OTP provides evidence of device possession to the bank, which may be an incredibly effective barrier against internet attacks.

ATM machines can also be used to conduct transactions. Biometric cards can only be used in ATM machines that are specifically designed for this purpose, as ATM cards must be fully inserted into the slot. For this, we can use two-factor authentication with a pin and an OTP. After inserting the card, users must authenticate using their secret pin. Additionally, an OTP is delivered to the user's phone, which is utilized in the second step of the authentication process.
After each transaction, an SMS is delivered to the user's phone, alerting them immediately if someone suspicious, debits or credits their account.

After each transaction, an SMS is delivered to the user's phone, alerting them immediately if someone suspicious debits or credits their account. Using these layers of fingerprints, pins, OTP, and SMS multi factor systems, we can provide an acceptable authentication approach to allow user transactions.

Case 2: Suggest certain areas in which biometrics would prove disastrous.

Biometrics is the study of people's unique physical and behavioral features through measurement and statistical analysis. The technology is mostly used for identification and access control, as well as identifying people who are being watched. The underlying idea of biometric authentication is that each individual can be reliably identified based on physical or behavioral characteristics.

Biometric identifiers such as fingerprints, hand form, vein pattern, facial structure, iris, blood, saliva, voice, heartbeat, signature dynamics, and many others are examples. All biometrics, regardless of type, share human characteristics. Biometrics (facial or fingerprint) rely on statistical algorithms despite the fact that they are unique and cannot be faked. We can't say it's 100 percent trustworthy.

Identifiers used in behavioral measurement include voice recognition, signature dynamics, keystrokes, and the sound of steps. Stress, disease, age, mental health, or emotions can all affect a person's behavior. Let's imagine we wish to use Google Assistant to unlock our phone with our voice. We can't say the same word with the same emphasis on the sound when we do this.

Our voices change as we get older or get sick. We're no longer able to use our phones. The rejection rate may be high in such instances, but the risk is modest. Nuclear power facilities, on the other hand, pose a substantially higher danger. Behavioral biometric IDs, as a result, are unsuitable for this application.

Replacing a malfunctioning biometric feature, on the other hand, is rare. This is compounded by the fact that a single biometric characteristic may be used by many systems, and flaws in one system may make the biometric feature less effective in another. Furthermore, such characteristics are not hidden; they are visible in our daily lives.

Using their fingerprint, only authorized personnel may have access to sensitive information, and it also produces a concrete audit trail of each transaction. Insider fraud is eliminated through the use of fingerprint biometric technology, which also promotes accountability and government compliance. Fingerprint authentication gives incontrovertible proof of employee and consumer interactions, potentially saving millions of dollars in financial fraud each year.