The Different Identity Verification Methods and How You Can Use Them In Your Institution

Identity verification is a crucial part of the success of today's businesses, especially for financial institutions and e-commerce companies. Anti-Money Laundering (AML) and Know Your Customer (KYC) are significant drivers in the development of identity verification techniques in the world. Each country has its organization and body that enforces these rules. In Nigeria, for example, the National Identity Management Commission is responsible for regulating identity verification methods.

What Is Identity Verification?

In understanding the different verification methods, it is crucial to know what identity verification means. Identity is the set of unique traits and characteristics associated with a unique and irreplaceable individual.

Identity verification ensures that there is a real person behind a process and proves that the individual is whom they claim to be, preventing both a person from carrying out a process on another individual’s behalf without authorization, and creating false identities or committing fraud. This is essential, with social media becoming a global medium and the rising cases of fraud. Identity Verification is required in most online and offline processes and procedures, from completing bank transactions to identification for international and national purposes.

There are various ways in which identity verification can be performed. In this article, we will go through the 4 conventional methods available to businesses today.

Knowledge-Based Authentication (KBA)

The knowledge-based authentication method allows a person to verify their identity by answering security questions, which only that person should have the answers to.

These questions are generally designed to be easy for that person to answer, but difficult for everyone else to answer. As an additional safeguard for this method, a time limit is given to specific questions. An advantage of this method is that it's user-friendly, which means it is the easiest for users to understand. Its most significant disadvantage is that it is getting easier to discover the answers through social media and other forms of social engineering. Another problem is that it does not rely on any government-issued identity, so any person with access to these answers can take undue advantage. This method can be used by online banking portals when transactions need to be completed and accessed, in ticket sales, where attendants try to verify who the people are, before the end of a transaction. Institutions that use this method expect that only the person who should know the answer will know the answer. Given how personal the question is, the user will have no problem recalling the correct answer.

Two-factor Authentication (2FA)

Two-factor authentication, also known as two-step verification or dual-factor authentication, is a verification process whereby users provide two different authentication factors to verify themselves. This method requires the user to provide a password and a security token or biometric factors such as fingerprint and facial scan before they can access an account.

This verification method makes it difficult for attackers to access a person's account because it goes beyond a password. Two-factor Authentication is particularly useful for creating and accessing accounts and resetting passwords. However, this method typically requires users to have their smartphones with them during the authentication process. Financial institutions, telecommunications, and school portals use this extra layer of security, a Time-based One-time Password (OTP) is sent either through SMS or generated using a Token. The user is required to input the generated password into the designated field to access their account.

Biometric Verification & Authentication

Biometric features are physical and biological characteristics that are unique to a person. Biometric techniques include facial recognition, voice recognition, iris, and retina scanning, and fingerprinting. If the biometric features of a user trying to access a device match the characteristics of an approved user, access to the device is granted. This method gives the user convenience as no password needs to be remembered or questions need to be answered. However, like other methods, this method also has its disadvantages. With the increasing rates of social media, voices can be recorded unknowingly. Which means some form of biometric information can be stolen. Databases can also be hacked to retrieve fingerprints. And once these types of assets are in the hands of an impersonator, it gets easier to defraud some institutions.
Both private and government institutions use this method for attendance capture. Financial institutions also use it for confirmation of a person's identity before a transaction is authorized while Consulates use this method for data capturing and verification.

Credit Bureau-Based Authentication

The credit bureau-based authentication method collects information from one or more of the major credit bureaus. These companies store credit information on consumers which includes, names, addresses, and in some cases, social security numbers or national identity numbers. This method uses a score to create a final match without compromising the user's experience. Financial institutions use this method to verify a person's identity, credibility, and track record.

The credit score is collated over time by a credit bureau and is made available to various financial institutions to help them make financial decisions such as granting loans, making investments, and trading. Credit scores can be used for risk assessment during employment vetting and background checks. Also, apartment leasing agencies assess an individual's credit score before making the leasing decision.

In conclusion, businesses and financial institutions rely heavily on the convenience of users. However, an effective verification method needs to be adopted to safeguard and protect the user experience. When choosing a verification method for your institution, be sure to use a technique that will draw information from multiple sources without compromising customer experience and security.