SPOTLIGHT

Sponsored by: Capgemini

Digital identity is an emerging solution that is attractive to financial services offering the capability to simultaneously meet regulatory requirements and align with business objectives.

The Value of Secure Digital Identity Controls

February 2024

Written by: Sean O'Malley, Research Director, Worldwide Compliance, Fraud, and Risk Analytics Strategies

Introduction

The identity of a person or entity has always been of the utmost importance in financial services. In banking, capital markets, insurance, or lending, confidence in the identities of the other parties involved is fundamental. Confidence is at the core of financial services, and being certain about the legitimacy of the person or entity with which you are engaging is crucial.

However, there are other concerns that also come into play with respect to identity. In many instances, the verification of identity is dependent on a set of data criteria that is commonly used to confirm an identity — name (either of a person or business), government identification number (such as a social security or passport number), registered address, date of birth (or incorporation for businesses), and so forth. This set of data criteria can be used to uniquely identify a person and is referred to as personally identifiable information (PII).

AT A GLANCE

KEY STAT

Identity fraud is the most common type of fraud, according to the U.S. Federal Trade Commission (FTC). The FTC reports that identity fraud has been the number 1 fraud type for over three years.

KEY TAKEAWAY

Growth in digital business transactions make it increasingly important to have reliable and secure digital identity processes and controls.

We delve into the challenges linked with these data criteria and investigate the strategies used to handle these complexities within the financial services sector.

As stated previously, data criteria play a crucial role in the process of identity verification, but it is important to understand the careful balance between needing these criteria and respecting the privacy concerns of individual customers. In many jurisdictions, legal/regulatory privacy frameworks demand strict privacy protection for personally identifiable information.

One of the vulnerabilities of verifying identity through data criteria is that anyone with access to this set of data criteria can misuse it to steal the identity of a person or business and engage in illicit activities or fraud.

Based on data collected by the U.S. Federal Trade Commission, the most significant type of fraud is identity fraud. Identity fraud — where someone uses the identity of a person or business through impersonation — has been the top type of fraud reported by the FTC for the past several years.

Many financial institutions maintain databases with customer data, and many of those databases contain data that can uniquely identify a person or business, including PII for individual customers. Cybersecurity serves as a prevalent strategy employed by financial institutions to safeguard and secure valuable customer data. This helps prevent unauthorized access to such information, making it more challenging for individuals with malicious intent to impersonate the institution's customers and attempt to gain control over their accounts.

Beyond relying on cybersecurity, financial institutions have undertaken other methods to enhance customer identity verification to ensure account access is granted only to the rightful person. Some institutions utilize biometrics, such as voice recognition, facial recognition, and fingerprints, to help in the customer verification process. Unfortunately, recent developments around generative artificial intelligence (GenAI) has made it easier for fraudsters to leverage GenAI voice technology that can circumvent the voice recognition controls and GenAI face technology that can circumvent facial recognition controls. This presents new challenges to security.

While there are many initiatives to create a digital identity that can be verified exclusively by the authorized account holder at a financial institution, the rising number of challenges poses difficulties in effectively preventing unauthorized access and exploitation by fraudsters.

As the speed of transactions accelerates, with an ever-increasing proportion of transactions occurring in real time, the importance of verifying the identities of the parties to a transaction becomes more crucial. The other complication to some real-time transactions is the involvement of nonhuman transactors, such as machine-to-machine interactions, introducing complexity to the process of identity verification and use of digital identity.

Definitions

The concept of digital identity evolved from the desire of businesses to authenticate the identity of their customers. The primary goal was to avoid being deceived by fraudsters who frequently use gathered information to adopt the identity of a customer associated with the institution.

Digital identity is defined by IDC as the utilization of information by computers to represent an individual or entity. Increasingly, the methods of digital identity are shifting toward solutions that minimize or eliminate the reliance for PII by relying on a broader range of data sets than those containing the data elements typically collected by financial institutions.

Benefits

When determining the most effective way to leverage digital identity for addressing business needs, it's important to consider several of the available alternatives and controls to be used in conjunction with digital identity to mitigate or avoid instances of identity fraud. However, the array of available alternatives and controls in this landscape can be highly complex and confusing to navigate. It is often advisable to approach this complex landscape in collaboration with a knowledgeable partner that can offer guidance regarding which alternatives and controls are best suited to address the needs of specific institutions.

A widely employed method for confirming the identity of a person or entity is multifactor authentication. It requires multiple verifications — often including one that is time sensitive — and is designed exclusively to provide information through a mechanism previously authorized by the customer. Access is granted to the customer only when all verifications are accurately completed and within the specified time frame. This control can be useful to help prevent certain types of identity fraud.

We have also seen the emergence of independent external consortiums (in some instances, companies) that conduct identity verification on behalf of their members or participants. Entities are not a subsidiary of the financial institution or business. They have financial institutions and businesses as members or participants that have contracted with the external consortium/company to ensure digital identity verification of the customer interacting with the financial institution or company. These entities have proven successful in reducing the instances of identity fraud and, in some cases, offer additional services such as identifying potential marketing targets for the products and services of the financial institution or company among their existing customer base.

Trends

Several trends are increasing the focus on digital identity. Identity fraud incidents are on the rise, leading to record-high losses attributed to identity fraud. Simultaneously, cybersecurity incidents are increasing, with malicious actors frequently targeting institutions such as banks to access PII and other highly valuable customer data that can then be used for illicit purposes.

Other concerning trends with respect to identity security include the increasing availability of new technological tools, including those powered by generative artificial intelligence. Fraudsters and money launderers can use GenAI tools to circumvent certain controls around identity authentication, particularly voice recognition and facial recognition controls. This circumvention of controls designed to help correctly identify humans in transactions becomes more challenging due to the increasing number of transactions that involve nonhuman interactions (machine to machine). The ability of fraudsters and money launderers to remain anonymous is heightened when the transactions are exclusively conducted between machines.

The proliferation of regulatory requirements is significantly impacting digital identity, particularly those rules regarding operational resiliency, cybersecurity, and data privacy. In the European Union (EU), a new regulatory requirement will take effect on January 17, 2025: the Digital Operational Resilience Act (DORA), which sets standards and requirements for operational resiliency and cybersecurity. Other jurisdictions, such as the province of Ontario in Canada, are following suit with respect to operational resiliency and security regulations. Data privacy has been a primary focus of regulatory authorities in a number of jurisdictions — especially in Europe with the General Data Protection Regulation (GDPR), which went into effect on May 25, 2018. In the United States, the Federal Reserve Bank's Privacy of Consumer Financial Information (also known as "Regulation P") governs data privacy for consumer information.

An additional trend that is impacting digital identity is data governance, which has been in place since the U.S. regulations passed after the financial crisis (2007–2009). Data governance focuses on data integrity, setting standards for data quality used in financial institutions. Many financial institutions have spent significant amounts of money in an overhaul of their technological infrastructure and data management efforts to meet a raft of data governance rules.

Considering Capgemini

Capgemini is a leader in the digital identity space offering advanced solutions in identity and access management (IAM). The company's offerings prioritize security, user experience, and compliance, aligning with key directives such as Network and Information Security Directive 2 (NIS 2), the Digital Operational Resilience Act, and the General Data Protection Regulation.

Leveraging its deep industry expertise, Capgemini integrates these directives into its IAM solutions, which are designed to ensure compliance with specific regulations and proactively adapt to evolving industry standards. This approach empowers organizations with a comprehensive and resilient framework for seamless and secure digital identity management in a dynamic regulatory landscape.

Challenges

There are a number of challenges around digital identity solutions and approaches. Balancing these challenges to achieve the desired business outcomes will require careful consideration, especially given the complexity of the issue and the rapid evolution of technology. As a result, unforeseen issues may arise that need to be addressed later.

IDC believes that the market for digital identity solutions will continue to evolve and expand in the near future across not only financial services but also other industries.

Conclusion

The combination of the trends mentioned previously is influencing the drive toward technical solutions and methods that either limit or eliminate the use of PII. These solutions aim to enhance operational resiliency and cybersecurity, streamline data privacy requirements, and align with the data quality standards established by regulators and sought by financial institutions. Navigating the solutions landscape, given these numerous and sometimes conflicting priorities, can be particularly challenging for any financial institution. It is often best to seek assistance from a provider with extensive expertise in guiding financial institutions through the digital identity maze.

About the Analyst

Sean O'Malley, *Research Director, Worldwide Compliance, Fraud, and Risk Analytics Strategies*

Sean is a compliance and risk executive thought leader with significant financial services experience. He has a track record of innovation and leadership in know your customer, anti–money laundering, OFAC/sanctions, compliance, transaction monitoring, enterprise risk management, operational risk, and risk assessments at top tier financial institutions.

MESSAGE FROM THE SPONSOR

Capgemini believes that digital identity will be at the heart of all digital interactions between public and private sector services across the globe. Industry knowledge, interoperability and open standards are essential towards the scaling of digital credentials.

At the same time, digital identity is under a growing threat due to new technologies. Bringing the best in cybersecurity solutions to secure digital identity and keeping pace with the developments in this space is key.

Scalable and trusted digital credentials will transform the way individual identities are managed. It goes without saying that Capgemini is committed to this.

With our Identity & Access Management (IAM) services, you can manage cyber security risks and gain control of new ways of working.

Learn More: https://www.capgemini.com/solutions/identity-access-management/

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com