Understanding digital identities in the world of cybercrime and compliance

Standard Chartered

What is it and why is it relevant?

A considerable part of our daily activity is composed of interacting with technology—online shopping, banking, social media, news updates, and fitness, to name a few. To conduct business, interact with other people, and meet personal needs, we use computers and other electronic devices to represent us in the digital world. The echoes of our interactions with the digital world, combined with the unique characteristics of each of the devices we use as interfaces (known as device fingerprints), can be used to create an online identity that corresponds to our physical person, known as a 'digital identity'. The uses for digital identities are numerous and expanding rapidly, and have many applications for financial institutions. For example, for fraud prevention, the identity of the customer can be confirmed by verifying the digital identity associated with that customer, rather than requiring the customer to answer additional questions or enter a one-time-password (OTP) received via email or phone. Inversely, digital identities can be developed for cybercrime actors based on their online activity, allowing financial institutions to proactively prevent attempts at account takeover or new account fraud.

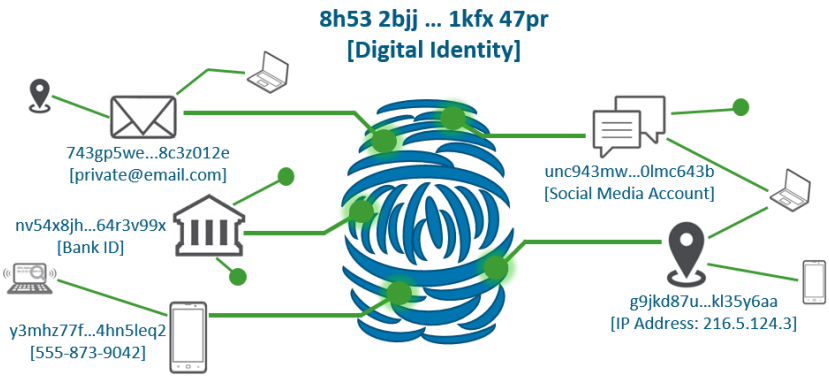
The digital projection of your physical space

A digital identity is composite record of multiple connected and related digital attributes, usefully associated with traditional personally identifiable information (PII). Each device we use (i.e. computer, smartphone, tablet) has associated 'attributes', such as media access control (MAC) addresses, registry settings, file locations, internet protocol (IP) addresses, associated email addresses, and so on.

The attributes for each device a person uses can then be compiled into an aggregate 'digital identity', uniquely identifying the person in the digital world. Digital identities are not static associations, like a social security number associated with a name. Rather, they are a dynamic combination of unique parameters derived from the 'device fingerprints' that can evolve with changes to the person's digital profile, and are thus very difficult to spoof or fake.

- **Financial services and other businesses** currently use static PII (i.e. date of birth, SSN) to identify an individual. For authentication purposes, for example, when someone needs to reset a password, firms will ask for the last four digits of the SSN and date of birth. However, it is increasingly likely most common static PII have been compromised and are available for sale on the darkweb, so the value of this method of authentication is dubious.
- **Financial institutions** using digital identities and dynamic PII in combination with static PII such as SSNs are better positioned to accurately authenticate a customer, and conversely, to defeat cybercriminals and fraudsters. With the major compromises of static PII through data breaches at medical insurance companies, consumer credit agencies, human resources vendors and so on, well-designed and vetted digital identities may be one of the best ways to protect both customers and financial institutions from fraud, identity theft, and the associated regulatory and compliance risk.

Examples of potential applications for Financial Crime compliance



Attributes of a digital identity considered PII, such as email and IP address, can be cryptographically hashed for privacy and security. The alphanumeric hash code is unique and irreversible, as even a change in capitalization in an attribute will produce a completely different hash value. This allows the indecipherable hash value to be sent across the internet, rather than the true value, making interception or fraudulent use of the digital identities components much more difficult for criminals.

The one-way encryption of digital identity attributes has enormous potential for information sharing between private sector partners for the prevention of fraud and the proactive prevention of cybercrime. Hashing of PII also enables vendors and non-profit partners to conduct aggregated analytical services without violating privacy laws or compromising customer data. If a digital identity is requested by law enforcement, the hashed values would need to be accompanied by the unencrypted customer information, which can only be provided by the owning financial institution.

Know Your Customer (KYC): Digital identities can be used in combination with email addresses, mobile numbers, and physical addresses to streamline client onboarding and enhance KYC compliance. For example, when opening an account, the financial institution (FI) can determine if the PII provided matches the individual's digital identity, including geographic location, device fingerprints, and previously used name, physical address, and so on. Alternatively, the FI can determine if the digital identity of the prospective customer has been previously associated with different PII, i.e. different names, physical addresses, and so on. This can be very helpful in identifying and preventing potential money mule activity, as well as preventing new account fraud.

Sanctions and Enhanced Due Diligence: When conducting due diligence, unraveling the ownership of a business can also be streamlined using digital identities. For example, the digital identity of a business owner may include details that reveal an association with a sanctioned entity, or IP address geolocation in a sanctioned country. Digital identities can also be used to unravel shell company activity by correlating device fingerprints with multiple businesses and activities that would otherwise be obfuscated.

Financial Cybercrime Red Flags: Digital identities can be used to identify and prevent certain types of cybercrime, by flagging those identities that have been associated with cybercrime activities, or that have been given a higher risk score due to involvement with money mule activities. Deviations from behavioral patterns compiled as part of a digital identity can be utilized as red flags for further review, and can also provide advanced notice of possible account takeover fraud or the compromise of customer credentials.