REPRINT

R&C risk & compliance

DIGITAL IDENTITY TO FIGHT FINANCIAL CRIME

REPRINTED FROM:

RISK & COMPLIANCE MAGAZINE

JUL-SEP 2019 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request a free copy of the full e-magazine

IdentityMind

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

ONE-ON-ONE INTERVIEW

DIGITAL IDENTITY TO FIGHT FINANCIAL CRIME

Jose Caldera
Chief Products and Marketing Officer
IdentityMind
T: +1 (650) 618 9980
E: jose@identitymind.com

Jose Caldera is chief marketing and products officer at IdentityMind, and has been developing and marketing high technology products for the last 25 years. An entrepreneur at heart, his focus has always been on the enterprise, developing products and services for information and payments security, risk mitigation and compliance. A frequent industry speaker and writer, Mr Caldera started his career in application and network security, later moving on to payments, virtual currencies, anti-fraud and anti-money laundering. He has developed and marketed products for a number of Silicon Valley companies including Securify, McAfee and IdentityMind.

R&C: Could you provide an overview of how digital identities are being utilised to tackle financial crime?

Caldera: The most difficult thing in financial crime is being able to track an individual, the many layers that may be used to hide their identity and the connections to other individuals or businesses. The addition of online financial business models and applications has further complicated matters, as online activities are easier to anonymise and much easier to hide the true identity behind the transactions. A proper digital identity infrastructure will allow the tracking and analysis of true identities of individuals, their connections and their activities in a much more accurate manner than today's analogue version. The usage of digital identities is in its infancy in financial crime detection. Most of what is implemented at the moment is the digitalisation of existing processes. If before, say, you went into a branch to open an account, now the documents can be digitalised and the verification of such documents performed online. Another example of current usage is your mobile phone as a proxy for identity. However, one cannot confuse the use of proxies and aggregation of transactional data being digitalised with the ability to track individuals with a digital construct that represents an identity. Building and maintaining a digital identity is the starting point. An adequate digital identity should represent the 'analogue' offline world and the 'digital' online components of an identity. It needs to be updated in real-time so that the latest changes are recorded in the identity. A digital identity has to be annotated in the context of the applications that are being used. The details of an identity for healthcare and insurance are certainly different than those needed for financial crime analysis. Digital identity needs to define and describe the authentication context required to succeed in an authentication or authorisation challenge, it has to be non-repudiable once it is established, and it has to be auditable by regulators and law enforcement. Furthermore, it has to be accessible at all times and informed by as many players as possible. There are many of us pushing the envelope, and pushing the industry to start adopting infrastructures with these features even within contained environments.

R&C: What factors are driving the growing interest and appetite to utilise this technology? How much are regulatory developments contributing to investment in this area?

Caldera: There are many factors, including the move toward online financial applications and the growth of alternative financial infrastructures, such as virtual currencies, alternative lending, and peer-2-peer payments. The inadequacy of identity-proofing mechanisms is exacerbated by

the easy access to private identity data, and the data needed to subvert the most used mechanisms of identity verification. As we spend more time online, more and more of our financial activity is there. This presence can be captured, analysed and utilised for enhanced analysis of individuals. The 11 September attack changed the scope of analysis and enforcement associated with money laundering, especially as it was used for financing terrorism, but the focus gave much-needed visibility into all nefarious activities that go through money-laundering techniques. The ability to process large quantities of data in finite time has enabled artificial intelligence (AI) and machine learning (ML) analysis at a very reasonable cost, especially when compared to the human resource cost. Regulatory mandates are in place to make sure the true individual owner behind a transaction is known. Both the US and EU have explicit mandates. Screening individuals and businesses against published lists developed and maintained by governments is required, and strong enforcement actions and regulatory fines may be issued when screening is not accomplished in a reasonable manner. And finally, aggregated regulatory mandates lead to expensive processes because they have been staffed with people. The availability of capable technology helps to curb the cost of compliance.

R&C: What are the benefits of adopting digital identity technology? Are there any challenges or pitfalls that typically surface along the way?

Caldera: We probably need to make a distinction between the current adoption of what is perceived as digital identities and what it can be. Some of the benefits are shared between the two, but the latter will have a more significant impact long term, than the current simple digitalisation of processes, because these are going online. Performing simple identity verification identities – like matching name, address and social security number (SSN) – can be performed automatically in real-time; there is no need for an operator or an analyst to perform a manual query. The verification of government identifications can also be streamlined and highly automated. Under current processes, the need for manual intervention can be largely reduced. The identity verification functions can be mostly automated, giving enough confidence to onboard customers and allow them to access financial services almost in real-time, allowing for monetisation of these clients much faster. The digital footprint left from the onboarding process and the interaction process allows for further monetisation of the clients. A digital construct that is available and capable of intaking information from different use cases and different parts of an organisation

can organise data in a way that enables analytics that are specific to the use. If the structure is globally accessible, it can be informed by other organisations. Reuse of digital identities across use cases and across organisations, or divisions within the same organisation, allows companies to make smarter decisions. It means that companies can reduce risk more quickly, or make the experience much better for good customers more quickly. The ability to capture an identity and the context upon which that identity can be further authenticated can be portable, enabling privacy features that can prevent data breaches and thereby eliminating many current, and envisioned, attack vectors. Furthermore, that portability can expand into authorisation assertions that can be utilised within and across organisations. A digital construct can be annotated and the authentication, verification and authorisation can be recorded in a transparent and auditable manner. There are pitfalls, however. One should not confuse a single function of the onboarding process as a true digital identity process. Point solutions provide a limited view into the identity, because they use small, niche sets of data to perform a particular function. In general, it does not build an actual identity that can be further tracked and enhanced. Also, going too big without being able to internally prove the value of the infrastructure generally creates too much discomfort for budget owners, and the change-management impact is hard to measure. The concepts and the benefits of adopting a true digital identity solution are still being documented and worked on. Very few providers have recognition from the industry, as the industry is yet to converge in taxonomy and definition surrounding the use of digital identities. The usual sources of credible data, like major analysts such as Gartner, Forrester and AITE, are catching up with innovators.

> **"Like with any other major technology shift, a project to change the core infrastructure of how you track and analyse individuals is not trivial."**
>
> *Jose Caldera, IdentityMind*

R&C: In what ways has digital identity technology improved in recent years and months? What innovations are enhancing available solutions against financial crime?

Caldera: The technology for extracting data from documents, and validating the security features of those documents, is becoming better and better. The use of AI and ML is accelerating this process. Moreover, the implementation of native biometrics in mobile devices, along with the adoption of mobile technology, is allowing for a very reasonable authentication mechanism. Finally, AI and ML are capable of taking large quantities of data and performing analysis that was difficult before. It is enabling automation of real-time processes and reduces the manual workload necessary. Not all processes can be automated and neither should we expect this to happen any time soon.

R&C: What steps should companies take to embed a company-wide digital identity management (DIM) system? What key issues do they need to consider?

Caldera: Like with any other major technology shift, a project to change the core infrastructure of how you track and analyse individuals is not trivial. The key aspects are to really understand your goals, understand what data is available, and understand how that data is going to inform your definition of identities and use cases. Make sure there is buy-in across stakeholders and that they see the benefits of sharing data through a common framework of identities. Start with a workable scope and grow from there.

R&C: How would you characterise the prevalence of fraud and money laundering across the globe at present? How might financial criminals seek to circumvent DIM systems?

Caldera: Going by available statistics, we are uncovering only 3 percent of money laundering worldwide. If the industry continues with the same current practices, nothing will change, because bad people will continue to exploit the financial system for whatever nefarious activity is profitable. We are behind in this race and we are losing. We have lots of work to do. Digital identities is a shift; it is the right one, but we are just starting. Building an infrastructure for compliance without considering digital identities is a mistake.

R&C: What themes do you expect to shape digital identity in the years ahead? Do you believe it will become an essential part of the toolkit to fight financial crime?

Caldera: Key aspects will be privacy, analytics and portability. These concepts are intertwined. Data breaches will continue and regulations, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CPPA), will have limited impact, because the reality is that users have become used to the benefits of vendors having

access to their data and behaviours. So the balance between services and privacy will continue to evolve. And it will converge into something we have not seen yet. A flip side will be portability of assertions of identities and regulatory processes, a solution that achieves both privacy – whatever that definition ends up being – and the ability to use and reuse that identity. This will drive the frameworks of identities that end up being adopted. The evolution of AI and ML will have an impact of the analysis of large amounts of data and uncovering complex schemes of financial crime that would otherwise have been completely invisible. More will be uncovered, and it will require human resource expertise in analysing all these findings, guiding law enforcement and continue to evolve regulatory frameworks. Blockchain presents itself as a natural framework for identity sovereignty, authentication and authorisation assertions that can enable auditability, transparency and privacy. I have zero doubts that digital identities will become a fundamental cornerstone to effective financial crime analysis. R&C