數位身份的現況探析

鄧靄儀*

摘要：在互聯網的時代下，數位身份 (Digital Identity) 的概念隨之而生。隨着數位交易的快速增長，以及受全球爆發新冠肺炎疫情的影響，經濟發展及社會生活進入新常態，雲端服務、遠程網絡和數位服務進一步普及。然而，數位化亦會帶來挑戰，例如增加了在線欺詐及身份盜用等風險，從而被犯罪分子利用，為了保障資料及交易的安全，各司法管轄區或國際組織制定相關規範或國際標準以應對數位身份產生的問題。現透過整理國際組織研究報告以及相關領域之論文，輔以網絡資源之蒐集，介紹數位身份之制度現況，探討相關優勢與風險，以及歸納現行數位身份技術在進行客戶盡職審查程序時的應用。在考慮推行數位身份制度之前，政府須建立完善的法律制度及資訊安全防護措施，並充分考慮新興技術帶來的固有金融犯罪風險程度，以應付數位交易的發展及變化。

關鍵詞：數位身份 身份驗證 清洗黑錢 客戶盡職審查

一、數位身份之定義

數位身份是由網絡空間存在的用戶個人資訊衍生而來的概念，數位身份是由一些特性或數位屬性組成的，利用數字化信息來對個人進行認別，即以數字代碼形式的公鑰或私鑰來代表個人的身份信息，從而可對個人的實時行為信息進行查詢及驗證。它是指描述用戶與網絡瀏覽器、行動應用程式和其他裝置各種互動過程中在線上建立和儲存的一組資料，或者是在網絡中可得的關於一個人的所有資訊之總和。網絡個人、組織或電子設備可能會通過不同的網絡社區，擁有不止一個數位身份。一個數位身份也可能和別的數字身份相關聯，比如電子郵箱、微博等。雖然這些與身份有關的屬性在一定程度上可以幫助確定一個人的身份，但是這些屬性是可以改變、隱藏甚至丟棄的[1]。

二、“基礎”身份系統與“功能”身份系統的區別

“基礎”身份系統：根據世界銀行的說法，數位基礎身份是“採取由上而下的方式所構建，其目的在於建立可以跨領域使用的通用身份識別，促進司法管轄區 / 地區發展”[2]。其提供者通常是司法管轄區或地區政府，他們希望為公民提供一種方式，以便透過身份證、戶籍登記冊、護照或出生證明來證明其身份。

“功能”身份系統：功能系統通常是旨在支援單一服務，如選舉登記、出生登記等。隨着技術的進步，一些新的方式正在取代傳統的紙本基礎身份系統，特別是在開發中地區。這使所有公民都能更輕鬆、更簡便地取得這些重要身份證件，尤其是一般上較不便利的新興地區。

---

* 鄧靄儀，金融情報辦公室顧問高級技術員，澳門大學工商管理學院市場學學士。

1. FATF, “Guidance on Digital ID, Financial Action Task Force (FATF)”, 2020.
2. The World Bank, “The World Bank Identification for Development”， https://id4d.worldbank.org/, 12 February 2022.

三、數位身份系統建立流程

(一)數位身份系統建立流程涉及兩個基本組成部分和一個選擇性組成部分:

1. 組成部分一:身份證明和註冊登錄(具有初始綁定/憑證)(必須);

2. 組成部分二:身份驗證(必須);

3. 組成部分三:可移植性和相互操作性機制(可選)。

身份證明和註冊登錄可以是數位化也可以是書面的,可透過面對面或非面對面方式進行。在數位身份系統中,綁定/憑證、身份驗證及可移植性必須是數位化的。不同司法管轄區和組織使用的術語可能會略有不同,這取決於所描述的系統。以下是每個階段的詳細說明。

組成部分一:身份證明和註冊登錄

身份證明和註冊登錄(具有初始綁定/憑證)共同構成了數位身份系統的第一階段。當身份資料與身份提供者所核發之憑證結合,再運用有效方式去驗證身份時,就可確認一個人是否具備他所聲稱之身份。身份服務提供者會收集、查驗和核實有關某個人的信息,以確認該指定人士是具備他所聲稱之身份。

組成部分二:身份驗證

身份驗證確定了準備登入帳戶(或其他服務)的個人與經過身份證明、註冊和認證並且擁有綁定憑證的控制權之人士為同一人。

組成部分三:可移植性和相互操作性機制

數位身份系統可以(但不是必須)包括一個允許可移植的官方身份證明。可移植身份是指互不相關的私人機構或政府部門與新客戶/市民建立關係時,可透過客戶/市民的個人數位身份憑證去證明其身份,而不必每次進行身份識別/驗證的步驟。

四、數位身份的識別與驗證[3]

身份識別(Identification)是為了判斷使用者是誰,而身份驗證(Authentication)是為了確保操作者的物理身份與數位身份相對應的步驟(例如:通過輸入密碼登入電子郵件信箱,或者利用生物辨識身份)。身份驗證主要的目標就是確認讀取系統的人是否為正確的使用者,這是確保資訊安全的重要環節,也是維繫數位服務順暢運作的重點。然而,不同的應用場景按其風險高低,為了在安全及便利中間取得良好平衡,其應用需要的身份驗證工具可能也有區別。

在現實環境,最常見方式是查閱身份證明文件;而在數位環境,則經常要求使用者輸入帳號及密碼。以金融機構的網上銀行系統為例,當使用者登入時,須輸入帳號或 ID (Identification) 等可供識別的資訊,系統便能確認"登入者"確實是帳戶擁有者本人,最常見而直接的驗證 (Authentication) 方式,就是要求使用者"輸入密碼"。

3. FATF, "Guidance on Digital ID, Financial Action Task Force (FATF)", 2020.

身份驗證技術所運用的驗證因素 (Authentication factors)，基本可分為三類：

1) 知識因素 (Knowledge Factors)

- 使用者知道的東西 (Something a person knows)，如：密碼、個人識別碼 (PIN)、挑戰應答認證機制 (Challenge–response) 等。

2) 所有權因素 (Ownership Factors)

- 使用者持有之物件 (Something a person has)，如：信用卡、提款卡、安全令牌 (Security token)、流動應用程式等。

3) 內在固有因素 (Inherent Factors)

- 使用者具有之形態 (Something a person is)，如：使用者的指紋、面容、虹膜等生物特徵。

自互聯網發展以來，許多政府服務、金融服務甚至醫療服務都延伸至網上進行，試圖在網絡世界實現可靠的身份驗證，令網上活動的可信性與實體活動處於同一水準，以促進更加安全和便利的網絡生活。金融科技 (Financial Technology，又稱 FinTech) 服務日漸發展，如銀行、證券、保險以及移動支付，都提供了不同的數位金融服務。但當我們想以簡單方便及容易操作的方式進行交易時，其實需要很多重要的措施配合，而身份驗證是關鍵因素之一。

五、數位身份的應用

數位身份目前最廣泛的應用是數位身份證 (eID) 及行動身份 (Mobile ID)。

(一) 數位身份證 eID

各個司法管轄區 / 地區都在努力制定智慧政府的藍圖，而數位身份證將是世界潮流。隨着 5G 時代的到來，移動設備與身份識別的結合更是未來的趨勢 [4]。

(二) 移動身份 Mobile ID

移動身份是一個相對較新的概念，仍處於起步階段，簡而言之，移動身份處理來自移動網絡運營商的資料，例如使用者的行動電話號碼 (MSISDN)、姓氏、名字、地址等。移動身份可以使用於智能手機或平板電腦等系統中，進行身份識別管理之技術。概念上可以包含面容辨識、指紋或聲紋等生物辨識方式，或者是某些裝置上利用使用者所擁有的資料的驗證方式等。總的來說，移動身份是數位身份的延伸，透過移動網絡或設備，它不僅是登錄和交易的推動者，而且還可以在與人和物的溝通與互動中發揮核心作用。移動身份可被視為一種安全及一體化的身份，應用在購物、旅行、甚至用於醫療保健和教育等重要服務 [5]。此外，移動身份只需要行動裝置，不需要實體卡，它可用於存取安全的電子服務，亦可對文件進行數位簽章，具有不需要讀卡機之特性，不過僅限於載有特殊 SIM 卡的行動裝置 [6]。

---

4. Trulioo, "eKYC– Electronic Know Your Customer best practices", 11 August 2022, https://www.trulioo.com/blog/ekyc/, 15 August 2022.
5. VERIFF, "What is mobile identity?", 3 November 2022, https://www.veriff.com/blog/what–is–mobile–identity, 15 December 2022.
6. Access Now, "NATIONAL DIGITAL IDENTITY PROGRAMMES: WHAT'S NEXT? P.9", https://www.accessnow.org/cms/assets/uploads/2019/11/Digital–Identity–Paper–Nov–2019.pdf, 6 April 2021.

六、數位身份的優勢與風險

(一)採用數位身份的優勢[7]

隨着數位身份的出現，令經濟社會的發展動力和發展方式產生深刻的改變，比傳統身份系統更有效提高整體社會效率，使政府、服務提供者及使用者等各方皆可從中得益。

提升政府與市民溝通的有效性	所有市民關鍵的身份資料和行為資訊均記錄在數位身份中，政府可因應不同屬性的市民及其需求提供相應的幫助。與此同時，監管部門亦能借助數位身份系統以強化及實施針對性監管，提升監管的有效性。
為使用者提供定制化產品和服務	透過系統中記錄的使用者身份資訊，服務提供者能針對不同使用者的屬性和目的以定制相應產品和服務。另一方面，數位身份系統可以在流程上有效取代以往複雜的紙本證書，降低服務提供者與使用者間反覆溝通的成本，從而提高辦事效率。
提升使用者使用個人資訊的靈活性	使用者不僅有權控制其他人對個人資料資訊的訪問，還可以決定發布自己資訊的時間、地點及方式。此外，個人身份資訊的數位化有助於使用者更方便地與外界進行交易，同時也能保護使用者遠離非法行為的影響。

(二)採用數位身份面臨的風險及威脅

1. 冒認身份的風險：

不能確定使用該數位身份的使用者是否為其本人，並難以從源頭上追溯系統中數位身份資訊的真實及有效性，更難以與網絡身份的真實性相對應。

2. 身份驗證和管理的風險：

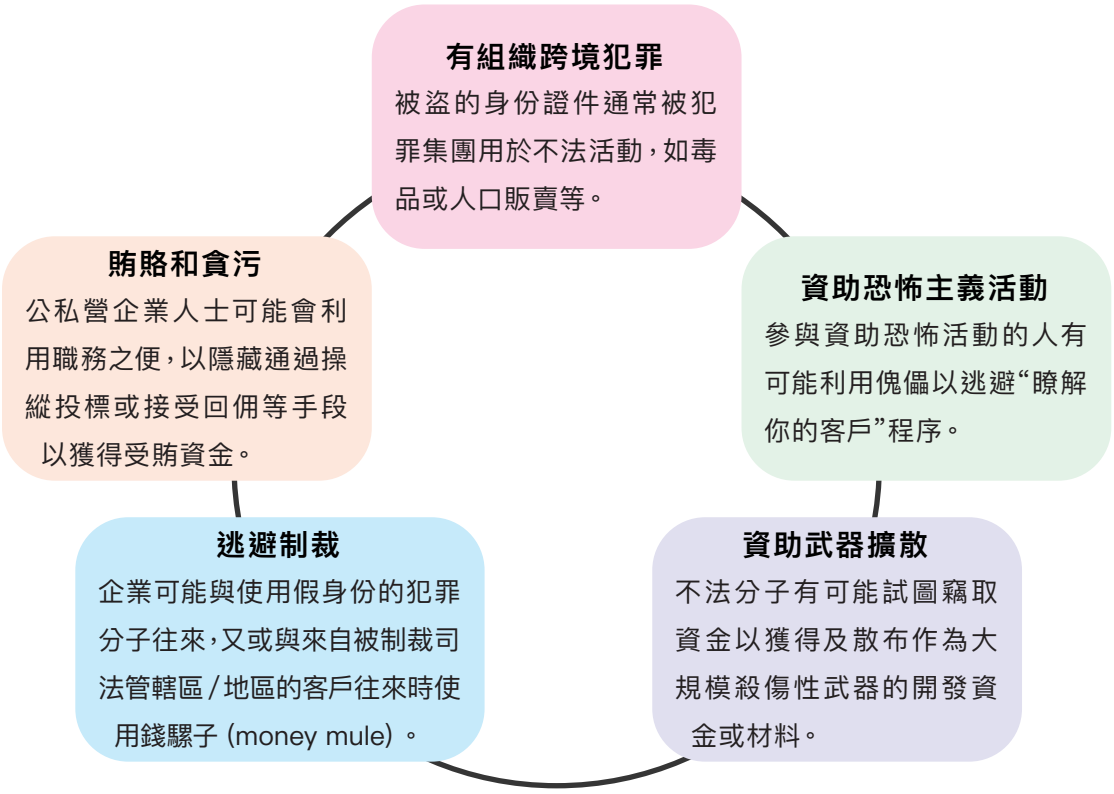
使用網絡服務的前提是要解決身份識別和認證的問題。如果身份認證方式比較簡單、效率不高，個人私隱資訊洩露的風險隨之增大，有可能導致使用者資訊被販賣，造成個人財產或其他利益的嚴重損失。

3. 資訊安全和私隱洩露的問題、來自網絡犯罪分子和駭客的威脅：

日漸增多的的駭客攻擊增加了資訊管理的安全風險。網絡犯罪分子試圖竊取敏感的身份資料，然後清洗不法資金（如：來自網上黑市販賣毒品所得資金）。此外，網絡犯罪分子和駭客試圖利用毫無戒心的個人和企業，竊取高度敏感的數位身份資訊，以達到有組織跨境犯罪、資助恐怖主義活動、資助武器擴散、逃避制裁、賄賂和貪污等目的。

---

7. 中國信通院 CAICT ，〈區塊鏈在數位身份的應用方向研究〉，2019 年 4 月 17 日，http://www.caict.ac.cn/kxyj/caictgd/tnull_197929.htm，2021 年 4 月 6 日到訪。



4. 清洗黑錢的風險：

遠端客戶開戶程序中需要考慮的一些關鍵因素包括清洗黑錢的風險程度，因為該程序缺乏面對面的交流，客戶可能會借助使用傀儡來掩飾帳戶持有人的真實身份。如果考慮到資料的私隱、網絡安全、欺詐、清洗黑錢、侵犯個人權利和自由，就會出現進一步的複雜情況。犯罪分子常用的一些清洗黑錢和隱藏帳戶實益擁有人的伎倆包括偽造身份、數位藍精靈（跑腿者）、使用匿名幣（如：虛擬貨幣，鑑於虛擬資產具有匿名買賣及無須經認可中央系統處理等性質，其日趨增加之交易對全球金融體系構成一定的清洗黑錢及恐怖融資風險）、利用線上網絡錢騾子、數位彈轉（在多個帳戶之間轉移資金）、增值（與微型分散交易相類似）、數位堆疊（使用電子錢包存儲價值）、化整為零（將資金分成幾部分並分散到不同的地點）等。

七、關於數位身份制度的國際標準與管理規範

隨着電子化的發展及科技的進步，數位身份的應用越來越多元化，無論是公共部門或私營企業的電子化服務或交易，對於身份驗證的需求越來越多，為了保障資料及交易的安全，各司法管轄區或國際組織制定相關規範或國際標準以應對數位身份產生的問題。目前國際上對於數位身份的管理及身份驗證頒布了不同的國際標準，以下將集中闡明金融行動特別工作組（FATF）數位身份指引之內容。

金融行動特別工作組客戶盡職審查及《數位身份指引》

金融行動特別工作組（Financial Action Task Force, FATF）成立於 1989 年，是七大工業國組織成員組成的政府間國際組織，為世界上打擊清洗黑錢的最重要國際組織之一。FATF 制定關於反清洗黑錢的《40 項建議》，對各司法管轄區立法以及國際反清洗黑錢法律制度的發展發揮了重要的指導作用。

因應新形態金融服務的出現，FATF 亦不斷修改其建議內容。隨着數位交易的快速增長，數位身份技術也正在迅速發展從而衍生出各種數位身份系統，如何在數位金融服務領域中識別和驗證客戶身份帶來了新

的挑戰。基於利用數位身份開展客戶身份識別的隱蔽性及便捷性高，潛在的清洗黑錢及恐怖融資的固有風險較高，因應數位化發展，解決新興支付方式所帶來的安全和透明度問題，FATF 於 2020 年 3 月發布了一份關於數位身份的指導性文件──《數位身份指引》(“Guidance on Digital Identity”)，對監管者、數位身份系統的使用者、身份提供者/開發商等提出了具體指導意見，指導了全球數位身份在進行客戶盡職審查程序時的應用，從而降低了因數位身份系統引發的清洗黑錢風險。可靠的數位身份可以讓識別程序變得更容易、更便宜和更安全，它還可以滿足交易監控要求並最大限度地減少人工監控措施中的弱點。

FATF 第 10 項建議已列明有關客戶盡職審查的要求，而 FATF 的《數位身份指引》指導性文件中亦有說明政府部門、受監管機構及其他相關機構如何以風險為本的原則透過數位身份系統識別及驗證客戶以符合第 10 項建議 (a) 項的要求，並同時能符合第 10 項建議 (d) 項關於持續客戶盡職審查之部分，當中主要包括下列兩大原則：

1. 瞭解數位身份識別系統主要組成部分的信用級別 (Assurance Level)（包括其技術、架構和管理），從而審視其可靠性及獨立資訊性；
2. 瞭解數位識別系統的信用級別後，進一步審視當中潛在的清洗黑錢、恐怖融資及其他不法金融風險。

在實務上，FATF 第 10 項建議及其註釋中要求受監管機構與客戶建立商業關係時，必須透過可靠及具獨立性的文件進行識別及核實工作，而 FATF 的建議中並不限制數位方式進行相關工作。然而，受監管機構必須以風險為本的原則進行客戶盡職審查，以減低潛在的清洗黑錢 / 恐怖融資風險。基於數位身份的識別及核實工作一般透過非面對面的方式進行，故此，應實施適當的反清洗黑錢 / 反恐怖融資風險緩減措施。有鑑於數位身份技術之進步，非面對面的客戶識別及交易若依靠獨立可靠來源的數位身份，並同時採取適當的措施以監控或降低風險，此情況可被視為一般風險等級；若實施更高的保證要求及 / 或配合適當的清洗黑錢及恐怖融資風險控制措施，便可進一步降低相關風險。

此外，根據 FATF 第 10 項建議 (d) 項，受監管機構必須對此類客戶進行持續業務關係盡職審查措施，以確保所進行的交易活動與機構對客戶的認知風險狀況保持一致。

八、鄰近地區運用數位身份系統的例子[8]

(一) 中國內地的個案例子：

數位身份系統是由私營部門根據經公安部驗證的客戶盡職審查資訊創建的，面容識別是通過與有效證件上的頭像進行匹配。每次驗證都是取得用戶的明確授權，並確認驗證服務的使用。

電子政務及電子商務於中國內地相當普及，並在不斷升級。例如支付寶、微信支付、無人超市、自助購票檢票、銀行的自助設施等，比比皆是。由於新一代科技的投入和普及，減輕了人工的工作量，縮短了辦事時間，提高了工作效率；減少或免除使用紙質文件，既環保又能降低成本。

8. FATF, “Appendix B in Guidance on Digital ID, Financial Action Task Force (FATF)”, 2020, ResearchGate, “The Imagination of Singapore’s Smart Nation as Digital Infrastructure: Rendering (Digital) Work Invisible”, 2019, https://www.researchgate.net/publication/336597152, 15 July2021.

（二）新加坡的個案例子：

新加坡的數位身份系統（National Digital Identity—NDI）是為當地居民和企業與政府及私營部門進行數位交易而建立的。NDI 堆疊中有 4 個不同的層次，即可信的資料、可信的身份、可信的訪問和可信的服務。雖然可信資料和可信身份層由政府提供，但可信資料是通過使用“Myinfo”制定的，其中包含 100 多個個人資料項目，金融機構將不需要獲得實物檔來驗證客戶的身份，也不需要單獨獲得客戶的照片。

（三）英國的個案例子：

英國主要開發了一個數位身份證系統，使公民能夠線上證明他們的身份。通過使用政府樞紐網絡（Government Hub Network）提供基礎設施，管理使用者、政府服務和私營部門身份供應商等之間的互動。

九、澳門特區的現況

身份證明局（DSI）是澳門特別行政區的政府機構，負責維護所有澳門居民的身份信息，由身份證明局提供的身份證明文件和身份識別數據資料屬獨立可靠的驗證來源。為方便市民使用智能身份證認證身份後進行各項電子化服務，身份證明局與其他政府部門或私人機構（如銀行）合作，透過技術協助以電子方式核實持證人身份，但所有相關的客戶盡職審查措施及程序仍屬相關機構的責任，並需由有關機構自行負責執行。

雖然上述驗證開戶方式屬於非面對面交易，清洗黑錢的潛在風險相對較高，但就開戶程序而言，現時身份證明局提供的身份驗證技術只限於本地居民，相關技術並不涵蓋非本地居民，因此不會影響或增加跨境清洗黑錢的風險。

隨着創新科技的快速發展，本澳越來越多機構透過應用新科技包括客戶遙距開戶，達到節省成本及改善客戶體驗的目的。然而，在利用科技帶來機遇的同時，機構應該有足夠的風險監控措施來控制相關的清洗黑錢和恐怖融資風險，以及可能出現被他人冒充等額外風險。

數位身份對於降低交易成本扮演關鍵的角色，各地區或許各自推動不同型態、技術的數位身份機制，但對現今科技的逐步信賴與加強應用，以及建構相關法規配套，已成為國際趨勢。

澳門特區政府近年不斷推進電子政務工作，隨着本澳第 2/2020 號法律《電子政務》及第 24/2020 號行政法規《電子政務施行細則》於 2020 年 9 月 27 日生效，為打造數字 / 數位政府，推動公共服務電子化提供了法律基礎，標誌着澳門特區政府電子政務進入新階段。澳門特區政府因應疫情帶來新的社會需求及挑戰，重新思考並調整電子政務的發展方向，認為應集中資源優先做好市民需求較多的電子服務。政府亦不斷優化雲計算中心基礎建設及管理制度，透過系統及網絡方面的升級，提高服務安全性和穩定性。為此，

澳門特區政府於 2019 年推出“澳門公共服務一戶通”(簡稱“一戶通”),澳門居民和實體均可開立“一戶通”帳戶,在統一網站平台或移動應用程式使用由澳門特區政府提供的各項電子化服務。為進一步強化澳門特區政府統一電子平台的建設,有效提高公共服務的便捷性,自 2021 年 9 月 21 日起,“一戶通”用戶可通過手機應用程式,將已持有的相關卡證綁定於“一戶通”電子卡包,範圍涉及醫療、教育、長者、職安、文康、環保等多個民生領域。此外,“一戶通”於 2022 年 4 月推出全面升級的 2.0 版本,服務主要仍集中在政府對居民 (G2C)、政府對企業 (G2B)、政府部門之間 (G2G) 及政府對員工 (G2E) 四種傳統基本模式,讓市民能夠更便捷地獲得所需要的服務和資訊,是次優化升級工作取得了一定成效,此乃為澳門跨範疇不同部門共同合作的成果,同時標誌着澳門特區電子政務發展踏上新台階。截至 2022 年 4 月,已有逾 33 萬人開立“一戶通”帳戶,“一戶通”所提供的電子服務數量也上升至 127 項。

十、結語

澳門特區政府陸續推出智慧城市與電子政務政策藍圖,多管齊下推動電子政務工作,實現提高行政效率、簡化行政程序及真正滿足社會發展需要,而數位身份亦是智慧轉型的基礎,隨着創新科技及人工智慧等技術的發展和成熟,數位身份認證將面臨更加複雜的環境,資訊安全的風險永遠存在,使得身份盜用和濫用成為數位身份的最大風險,如何保證網絡空間中數位身份的唯一性和安全性亦是至關重要問題。因此在考慮推行數位身份制度之前,政府須建立完善的法律制度及資訊安全相關的防護,提升使用者的信任,以及持續與市民溝通相關政策,為相關企業制定新的瞭解你的客戶和客戶盡職審查監管準則,簡化過時的客戶開戶流程,並充分考慮新興技術帶來的固有金融犯罪風險程度,才能跟上數位交易的發展,期許澳門特區在不久的將來也可以建立一套完善的數位身份制度,擠身先進數位地區之列。

參考資料:

1. FATF, “Guidance on Digital ID, Financial Action Task Force (FATF)”, 2020.
2. World Bank Group, “Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, A joint World Bank Group—GSMA—Secure Identity Alliance Discussion Paper”, 2016.
3. 包明友、吳雲:〈如何證明你是你?—數字身份識別在金融中的應用〉,《金融市場研究》,2020年,第96期。
4. Paul A. Grassi, Michael E. Garcia and James L. Fenton, “Digital Identity Guidelines,” National Institute of Standards and Technology, 2017.
5. Eugenio (Gene) DiMira, “Digital Identification Methods and Testing for AML Programs,” CAMS–Audit Advanced Certification White Paper, Association of Certified Anti–Money Laundering Specialists, 2021.