CAPCO

JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

SECURITY

E-residency: The next evolution of digital identity

CLARE SULLIVAN

DIGITIZATION

#47
04.2018

JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

ORGANIZATION

CURRENCY

SECURITY

E-residency: The next evolution of digital identity

CLARE SULLIVAN | Visiting Professor, Law Center and Fellow, Center for National Security and the Law Georgetown University, Washington D.C.

ABSTRACT

This article examines the next evolution in government-backed digital identity programs that enable public and private sector transactions by individuals. Estonia is the first nation to offer e-residency to individuals who are not Estonian citizens and who are not legally resident, or even physically present, in Estonia. The Estonian program is the first government-authenticated and operated, international digital identity program that enables remote-access international commercial transactions that range from establishing and operating a company, trading in goods and services, opening and operating a bank account, to buying and selling securities. While Estonian e-residency is designed to expand the economic base of Estonia beyond its geographical boundaries, and in that regard, it is successful and inspiring, its impact is much more profound and far reaching. In establishing e-residency, whereby anyone, based anywhere in the world, can do business and banking in Estonia, and then potentially in the European Union (E.U.) and elsewhere, Estonia is changing traditional approaches to immigration, residency, and international business. In effectively opening a new virtual domain, Estonia is redefining what it means to be a nation and a citizen in the digital era, and is challenging the very nature and scope of international commerce and finance, and of regulation based on physical boundaries.

1. INTRODUCTION

In December 2014, Estonia became the first nation to open its digital borders to persons throughout the world to become an Estonian e-resident. Estonia is the most advanced e-society in the world and is an acknowledged leader in technology innovation. The Estonian e-residency program is another example of the country's extraordinary vision and ingenuity. In launching e-residency, Estonia hoped it would be transformative and disruptive, and it has proved to be so.

The primary objective of the e-residency program is expansion of Estonia's economic base, which is limited by its geography and relatively low population of around one million inhabitants. Under the program, anyone, based, anywhere in the world, can become a virtual economic resident of Estonia. Estonia is a member of the E.U., so e-residency also facilitates broader commercial access to Europe.

When the program first launched, applicants had to go to Estonia to apply in person to become an e-resident and to open an Estonian bank account. Now, without ever setting foot in the nation, a person can apply to become an e-resident and obtain an e-ID issued by the Estonian government. Digital trust services, including electronic signatures and seals, and blockchain technology underpin the program to enable an e-resident to remotely access and use a range of Estonian e-government and private sector services. An e-resident is able to remotely perform a full range of commercial activities, including business and company registration and operation, banking (including funds transfers), buying and selling of real estate and other property, and trade in goods and services.

E-residents are subject to Estonian tax,[1] and e-residency does not operate as a tax shelter in relation to other jurisdictions. The e-ID issued to e-residents does not have the status of a passport or visa and does not automatically lead to Estonian permanent resident status, nor to citizenship in the traditional sense, although in a way it can be viewed as a new form of economic immigration. In establishing the program, Estonia has expanded its business and revenue base while keeping operational costs low. Estonia has opened new economic channels, created a new virtual domain for international commerce, and is fundamentally changing the nature of international commerce and finance.

2. A TRANSFORMATIVE SUCCESS STORY

The e-residency program has achieved its objective of economic expansion. The number of applicants for e-residency has grown steadily since the program launch, exceeding projections and expectations.[2]

There are currently 27,600 Estonian e-residents, who to date have established 4495 companies.[3] In a recent report, Deloitte estimated that e-residency has brought "€14.4 million in income, including €1.4 million in net income and €13 million in net indirect socio-economic benefits" to Estonia in three years.[4] This confirms the Estonian government analysis. The return on investment is estimated by the Estonian government to be €100 euros for each euro it has invested in the e-residency program.[5]

As has been the case since the inception of the program, Finland, Russia, Ukraine, and the U.S. have the largest number of Estonian e-residents. Overall, people from 138 countries have applied for e-residency.[6] There is now at least one Estonian e-resident in every corner of the world, making it one of the most expansive and comprehensive commercial networks in the world.

In the years following its launch, the e-residency program has developed rapidly in terms of number of applicants and the services available to them. New commercial services have been added through the Estonian government partnering with private-sector providers. Blockchain technology has been extended to identity authentication and verification, document authentication and management, payment systems, and new trading securities offered by NASDAQ, for example. Other developments include the establishment of eResNetwork, a new business networking platform for e-residents to communicate securely with other e-residents; and broader use of X-road, the platform used for both the e-residency program and e-Estonia services for physical residents and citizens, as a joint data exchange platform between Estonia and Finland.

---

1 Undistributed profits that are reinvested into the Estonian company are not subject to Estonian corporate tax.

2 Kaspar Korjus, the e-Residency Program Manager, reportedly stated in March 2017 that, "[It is] important for startups to set goals that are both ambitious and achievable. Our target of 10 million e-Residents will require exponential growth, but the early indications are that we are on schedule. We already have more e-residents than expected at this stage." As reported by Kalev Aasmae, "Estonia has 1.3 million people: Here's how it plans to get 10 million e-residents by 2025," ZDNeT, March 20, 2017, http://zd.net/2nQJWTa

3 Republic of Estonia, E-Residency statistics, http://bit.ly/1P68QaR.

4 Deloitte, 2017, E-residency brought €14.4 million to Estonia in first three years, December 2, http://bit.ly/2FVs3tL. According to this report, it is projected that by 2021, the program could generate €31 million in net income and €194 million in net indirect socio-economic benefits, assuming that Estonia will have 150,200 e-residents by 2021 who have established 20,200 businesses.

5 According to Kaspar Korjus, head of the Estonian e-residency program. See Deloitte (2017).

6 Republic of Estonia, e-residency, http://bit.ly/2BNJkqY

In 2018, Estonia also announced that it will be launching the first government-backed virtual currency, to be called Estcoin, to be used as part of the e-residency program. A number of approaches are under consideration. One approach is to use these "crypto tokens" to reward those who further develop the e-residency program, and refer new e-residents in furtherance of Estonia's objective of developing the digital nation. Another notable proposal is to use Estcoin for transactions by e-residents and perhaps others; and there are thoughts of pegging Estcoin to the Euro. Estcoin is seen as a means of reducing the costs involved in verifying identity for transactions and for avoiding cross-border banking fees for transactions among e-residents. The full implications are not yet known but it is clear that transactions using Estcoin will be blockchain-based and that this use of Estcoin will be a highly disruptive development likely to be also adopted by other nations.

3. BROADER SIGNIFICANCE

The relevance of the e-residency program extends beyond Estonia, as use of government-authenticated e-IDs for remote-access international transactions gains traction.

The Estonian program is setting the standard for similar international digital identity programs, most notably mutual e-ID recognition and data exchange between Estonia and Finland. Estonia, Belgium, Portugal, Lithuania, and Finland already mutually recognize their respective government-authenticated e-IDs for some transactions, and Estonia and Finland are further developing their interoperability using X-road, the exchange program used for e-residency, as well as e-services for Estonian citizens and physical residents.

The other major international development is the new "digital single market" (DSM) being established in the E.U. and the "single digital identity" (SDI) being established as part of that program. The objective of SDI is the mutual recognition of government-authenticated e-IDs between member nations to enable remote commercial transactions in the E.U. These initiatives are led by Andrus Ansip, a Vice President at the European Commission (E.C.), and the former Prime Minister of Estonia. Estonia's assumption of the E.U. Presidency in 2017 has further strengthened its influential role.

The Estonian e-residency program, its technology, and its commercial features are instructive for all nations and regions that want to expand their economic base without the security risks and costs associated with traditional immigration. In particular, the program offers many lessons for other nations in relation to new scope for economic expansion and development of international commerce and finance based on e-ID and blockchain technology. Many nations are considering the broader use of blockchain for identity management, for commercial and financial transactions, and for new cryptocurrencies.[7]

[7] Including, for example, the U.K., Australia, and the U.S.

By not defining itself by geography, but instead by digital capability, Estonia is re-writing what it is to be a nation in this era. By not defining economic participation primarily by physical location or birth, Estonia is changing traditional notions of residency and ultimately of immigration and citizenship, and is opening the way for universal e-IDs and global virtual economic citizens. In using blockchain as the basis of the e-residency program, Estonia is changing the way this technology has been used and is expanding its application to e-ID and a full range of commercial as well as financial transactions. In establishing new virtual services for e-residents, Estonia is substantially expanding commercial channels and is changing the nature of international commerce. In launching Estcoin Estonia is changing international finance.[8]

4. CHALLENGES

As the first international e-ID program, e-residency introduces new ways of doing business and new types of risk. Many of the features that make the Estonian e-residency program innovative and attractive to entrepreneurs also make it susceptible to misuse, especially for identity fraud, including the creation and use of new digital identities, transaction fraud, and trade-based money laundering. Estonia's start-up culture, which has had a notable impact on the development of the e-residency program from its inception, is of itself a risk factor. The Estonian government has candidly acknowledged that it is operating the e-residency program like a start-up and will address issues as, and when, they arise.[9]

The nature and magnitude of the risks largely depends on the accuracy, integrity, and security of e-program protocols and procedures, on its legal, regulatory and enforcement underpinning, and on the integrity of the program technology. A recent incident is illustrative. In December 2017, Estonia announced that it is upgrading the security of e-ID cards used by e-residents, as a result of a security vulnerability found in software installed on the embedded chip in cards issued between 16 October 2014 and 25 October 2017. The vulnerability affected cards and computer systems around the world that use these chips. The vulnerability in the chip on the e-resident e-ID made it possible for the e-ID to be misused, though Estonia has reported that it is not aware of any incidence where that occurred. The process for updating the certificates for the e-ID card as part of addressing the security vulnerability is proving to be slow, prompting Estonia to strongly recommend that in the meantime, e-residents use a private sector service called Smart-ID so that their business dealings can continue uninterrupted. Smart-ID is a mobile app that was launched in 2016 by SK ID Solutions, which is partnering with the Estonian government to issue certificates for identity documents held by e-residents, as well as Estonian citizens and physical residents. An e-resident can download the Smart-ID app to an Android or iOS phone and then only needs to authenticate his/her identity once using the e-ID card to access e-services.

Smart-ID can be used for transactions, signing agreements, and activating new cards for business banking and finance with LHV, an Estonian banking and financial services company; Swedbank a Nordic-Baltic banking group based in Stockholm, with a significant presence in Estonia; and with Leap IN, a business services provider that offers a turn-key solution for setting up a location-independent single-person company. While Smart-ID clearly facilitates business, it raises questions about the rigor of identity authentication and verification, especially for banking services that need to comply with the "know your customer" (KYC) and other monitoring and reporting obligations mandated by Anti-Money Laundering/ Counter-Terrorism Financing (AML/CTF) legislation enacted in most nations including Estonia following the 9/11 terrorist attacks in the U.S.[10]

Another move that raises similar concerns is a new one-step, one-time KYC process that will be used by Change Bank.[11] The bank will leverage the Estonian e-residency program's e-ID for identity authentication to quickly sign-up e-residents as customers for crypto-banking. Reportedly, this process requires only basic background information.[12] When an e-resident completes the simple one-step identity authentication, a multi-asset blockchain-based Change wallet is created, enabling use of cryptocurrencies by e-residents through a mobile app. A Change debit card allows e-residents to make payments and withdraw funds from ATMs all over

[8] See Republic of Estonia, "Estcoin: a proposal to launch the world's first government ICO," http://bit.ly/2EdsAHi.

[9] Siim Sikkut, ICT Advisor, Government of Estonia, "E-stonia – a startup country," Back Light, June 15, 2015 at http://bit.ly/2E8Tvnj

[10] The legislation generally mandates that banks and financial institutions check and report the identity of every customer. The KYC requirements demand that a person establish his/her identity to open a bank account usually through a face-to-face interview, at which time a birth certificate, passport, and other identity documentation is produced to authenticate and verify identity. The requirement for an initial face-to-face interview and subsequently for some specified transactions, is in line with the banks' obligations under Good Banking Practice, the Estonian banking code of practice, and with AML/CTF legislation. See Good Banking Practice, Part 6, http://bit.ly/2BLvTI0. Although this is not legislation, as a code of practice it closely follows the KYC and STR requirements typically found in the AML/CTF legislation.

the world, using a crypto-to-fiat currency conversion. It is envisaged that e-residents will eventually be able to use the Change mobile app to invest in stocks, obtain peer-to-peer loans, and buy and sell real estate.

The e-residency program's collaboration for these broader uses of blockchain also raises concerns, especially for the blockchain-based services that are capable of operating outside traditional legal frameworks and existing international monitoring and enforcement regimes. For example, Estonia is collaborating with Bitnation, one of several emerging initiatives based on blockchain technology that are specifically designed to bypass traditional, national governance systems. In its broadest application, Bitnation aims to use blockchain to provide a new system to vouch for identity, for contractual agreements, including those for banking and company incorporation, and for new payment systems that operate outside regulated, monitored channels.[13] As the joint press statement points out, "[v]ia the international Bitnation Public Notary, e-Residents, regardless of where they live or do business, will be able to notarize their marriages, birth certificates, business contracts, and much more on the blockchain."[14]

According to Susanne Templehof, founder of Bitnation, the broad objective is "to gain recognition for Bitnation as a sovereign entity, thus creating a precedent for open source protocol to be considered as sovereign jurisdictions."[15] This, in effect, seeks to "establish a new virtual jurisdiction with its own rules."[16] The underlying philosophy is that identity is established using a distributed ledger on a global open source platform, rather than using traditional authentication sources like government records and authentication intermediaries like banks. This potential use of blockchain for identity authentication and verification, and for at least some transactions for Estonian e-residents, is a significant development that can enable the provision of self-sovereign identity and other related services to e-residents, outside exiting legal channels and protocols. The development and use of these under-governed and ungoverned domains for commercial activity also increases their potential use for illicit, destabilizing activity that has both national and international implications.

E-residency introduces considerable change to international commerce that can, by its nature, be destabilizing. However, expansion of the program into global trading markets by adding NASDAQ and into new blockchain-based services offered by Bitnation are especially impactful, because anyone with an Estonian e-residency ID can engage in trade in stocks, futures, commodities, and currency. These developments have implications for the stability and security of global commercial and financial markets, and security generally. Of particular concern is the use of these types of programs for concealing and funding terrorist and organized criminal activity and other illicit and destabilizing activities by rogue individuals, foreign powers, extremist organizations, and criminal networks.

These aspects highlight the need for rigorous new security protocols and procedures; and for these types of international digital identity programs to be based within an effective, robust national and international regulatory and security framework designed to address the new challenges presented by these programs. This is particularly so in view of the program's international reach and impact.

---

[11] Change Bank is based in Singapore and is licensed by the Monetary Authority of Singapore. http://bit.ly/2nL6Fko.

[12] Prisco, G., 2017, "Estonia partners with Change Bank for blockchain e-residency program," NASDAQ, September 28, http://bit.ly/2GVMNDb.

[13] Bitnation describes itself as "a decentralized, open-source movement, powered by the Bitcoin blockchain 2.0 technology, in an attempt to foster a peer-to-peer voluntary governance system, rather than the current 'top-down', 'one-size-fits-all' model, restrained by the current nation-state-engineered geographical apartheid, where your quality of life is defined by where you were arbitrarily born." In further detail, Bitnation states that it "provides the same services traditional governments provides, from dispute resolution and insurance to security and much more – but in a geographically unbound, decentralized, and voluntary way. Bitnation is powered by Bitcoin 2.0 blockchain technology – a cryptographically secured public ledger distributed amongst all of its users. As we like to say – Bitnation: Blockchains, Not Borders." See Bitnation Governance 02 at http://bit.ly/2sesq0d.

[14] Tempelhof's comments in relation to the collaboration with Estonia are more moderate: "[m]y aim is to see a world where hundreds of thousands or millions of governance service providers in a free global market competing through offering better services at a better value, rather than through the use of force within arbitrary lines in the sand." "To that end, seeing nation state governments starting to provide governance services on a free global market as well, like The Republic of Estonia, is encouraging, and a step in the right direction. Now we need more nation state governments, as well as open source protocols joining the global market." See Giulio Prisco, "Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents" Bitcoin Magazine, December 1, 2015, http://bit.ly/1OvfExl.

[15] As reported by Ian Allison, "Bitnation and Estonian government start spreading sovereign jurisdiction on the blockchain," 28 November, 2015, http://bit.ly/1OpDJpS. Bitnation has recently received international attention for providing assistance to Syrian refugees in Europe, including an emergency digital identity and financial services through a Bitcoin Visa card to enable a refugee who cannot establish a bank account to receive funds from family, for example. Blockchain is used to cryptographically establish an individual's existence and family relations to generate a digital identity. That identity generates a Quick Response Code, an optical label that contains information in machine-readable form that can be read by a mobile phone to apply for a Bitcoin Visa card, which can be used throughout Europe without a bank account. Susanne Templehof, founder of Bitnation, reportedly explained that "the Blockchain Emergency ID is a rudimentary emergency ID, based on the blockchain technology, for individuals who cannot obtain other documents of identification." She explains, "[w]e are providing emergency ID and then this visa card because most refugees will be unemployed. They won't be legally able to get a job for several years and they can't open a bank account." See Ian Allison, "Decentralised government project Bitnation offers refugees blockchain IDs and bitcoin debit cards" International Business Times, October 30, 2015, http://bit.ly/1RTRPR5. Use of blockchain in this type of situation to create an emergency, temporary digital identity to enable aid to be given to an individual who is unable to otherwise establish his/her identity may be admirable. However, it does raise security concerns, particularly in the use of this to create a new false identity and to engage in nefarious and covert activities ranging from crimes like money laundering to activities endangering national and international security.

[16] Ibid. As well as the huge increase in stateless people in Europe from the refugee crisis, Bitnation is looking at developing markets, assisted economies, and the grey economy. For example, the registry capabilities of blockchain are being considered as a means of recognizing land rights in the developing world, in countries like Ghana, where 70% of land is reportedly untitled and land is traded peer to peer.

A more comprehensive international approach is needed to establish a standard for the design and operation of these programs. Standards that currently exist are fragmented, tending to cover in depth either technical requirements,[17]or detailed procedural guidelines, such as those for banking, which are developed primarily at industry or sector level. As part of the DSM, the E.C is currently proposing a new E.U. Cybersecurity Agency and a certification framework to provide a set of rules, technical requirements, standards, and procedures. The focus, however, is on the E.U.[18]

The proposed certification is to attest that products and services are in certified in accordance with specified cybersecurity requirements, and will be recognized in all member states. This proposal is in its early stages so the time for implementation is not known, but it is designed to address areas of variability between member nations to facilitate trade across borders. It is also not yet clear how comprehensive or detailed the framework will be, but it is likely to be risk-based, in line with existing national and regional legal requirements that specify that there be appropriate technical and organizational measures to ensure a level of security appropriate to the risk to an individual's personal data. In line with the requirement in the E.U. to protect the fundamental human rights, the focus of the E.U. security requirements will primarily be on protection from unauthorized disclosure of the personal data, and privacy, of E.U. citizens and residents,[19] rather than on issues of concern to the broader international community.

Initiatives to address security issues are also E.U. focused. For example, the E.U. has recently adopted a framework for a joint E.U. diplomatic response to malicious cyber activities that sets out measures under the Common Foreign and Security Policy, including restrictive measures "that can be used to strengthen the E.U.'s response to activities that harm its political, security and economic interests."[20]

New transnational digital identity programs like Estonian e-residency and the E.U. DSM fundamentally challenge exiting regulation and enforcement, which is based on national law. The nature and broader effects of these programs require a coordinated international response. While these new e-ID programs raise new, more complex issues and concerns, the widespread adoption of the AML/CTF requirements is precedent for, and an example of, the type of international cooperation required and possible.

5. CONCLUSION

The next evolution of digital identity programs, like the Estonian e-residency and future iterations, have unprecedented implications for commerce, finance, security, international law, and legal norms, caused by the virtual dismantling of geographical boundaries and traditional concepts of immigration, residency, and even citizenship, based on birth and/or physical presence.

The technological, policy, and procedural vulnerabilities of this next evolution of digital identity programs impact both national and international security and stability. Identity fraud, fraudulent transactions, and money laundering, especially trade-based money laundering, are the most significant known risks. However, these types of digital identity programs and their data are strategic assets and potential targets that can be used by criminals and adversaries not just for known forms of identity fraud and money laundering, but for new, and as yet unanticipated, types of destabilizing and offensive activities. These programs have extensive international reach, with the Estonian e-residency program, for example, spanning the globe with potential operatives.

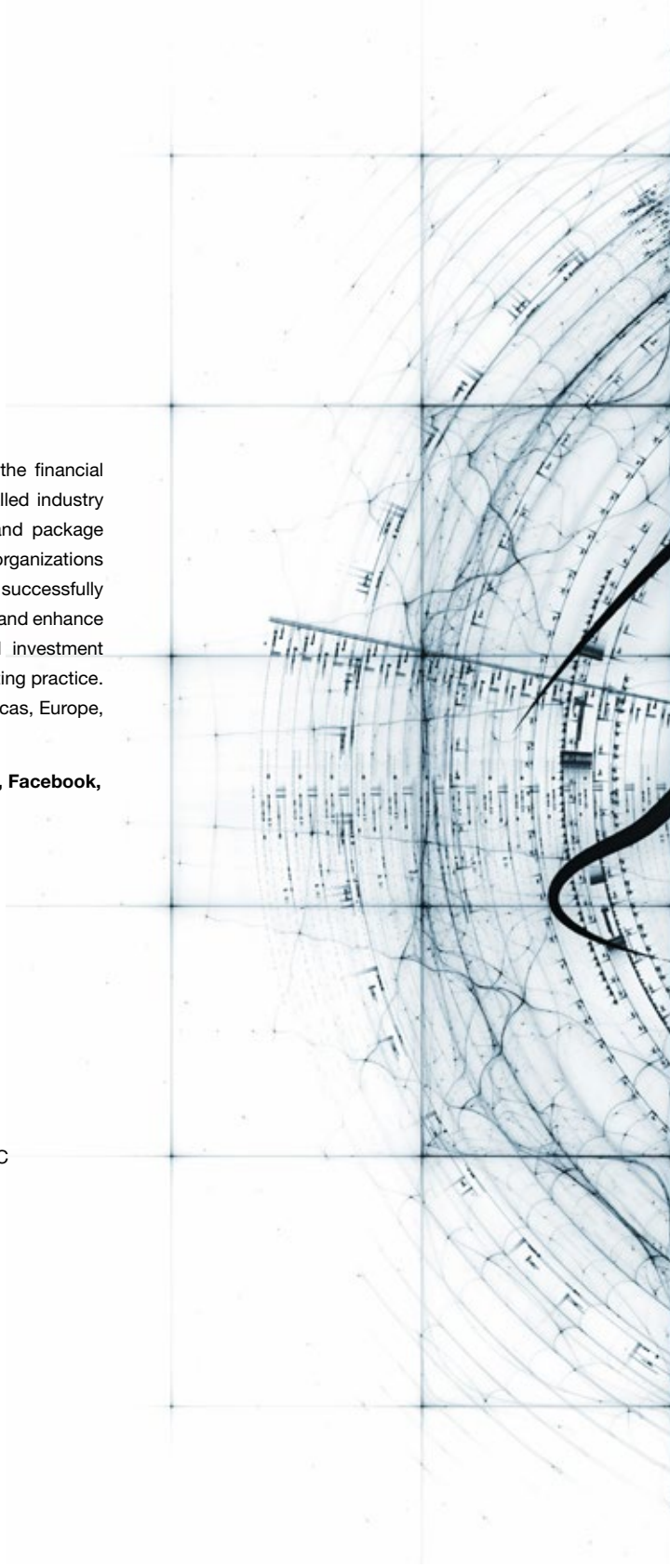
These new digital identity programs, of which Estonian e-residency is the current leader, offer many benefits to the host nation and to individual entrepreneurs, but they challenge the effectiveness of traditional regulation and, potentially, the stability and security of international financial and commercial markets. International coordination and cooperation is needed to ensure these programs meet international standards in their design and operation, particularly in relation to identity authentication at the time of program registration by an individual and, subsequently, for identity verification for transactions. International cooperation is also needed to establish a transnational framework for monitoring and regulating financial and commercial transactions, including those in currently under-regulated and unregulated channels and domains.

[17] The U.S. National Institute for Standards and Technology (NIST) technical guidelines for Federal agencies implementing electronic authentication is an example.

[18] See E.C., "Policies: digital single market: cybersecurity," http://bit.ly/2xAu7rq. See also E.C., "Digital single market, policies: the EU cybersecurity certification framework," http://bit.ly/2E9NOWj.

[19] For example, see Article 32 of the E.U. General Data Protection Regulation, which provides that "[t]aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk … account shall be taken in particular of the risks that are presented by processing … which could lead to physical, material or non-material damage" (my emphasis). Specific authoritative guidance is usually only provided in the event of litigation when a court may comment on requirements.

[20] The E.C. reports that "[i]mplementation work on the Framework is currently ongoing with Member States and would also be taken forward in close coordination with the Blueprint to respond to large scale cyber incidents." See E.C., "Policies: digital single market, cybersecurity, cyberdefense," http://bit.ly/2Eouubp.



ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward. Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, and finance, risk & compliance. We also have an energy consulting practice. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Xing.**

WORLDWIDE OFFICES

Bangalore
Bangkok
Bratislava
Brussels
Charlotte
Chicago
Dallas
Dusseldorf
Edinburgh
Frankfurt
Geneva
Hong Kong
Houston
Kuala Lumpur
London
New York
Orlando
Paris
Pune
São Paulo
Singapore
Stockholm
Toronto
Vienna
Warsaw
Washington, DC
Zurich

CAPCO.COM

CAPCO