WALKERS

Global Legal and Professional Services

Relying on Digital ID for AML/CFT Purposes in Jersey and Guernsey

August 2020

The financial services regulators in both Guernsey and Jersey – the Guernsey Financial Services Commission ("GFSC") and Jersey Financial Services Commission ("JFSC") respectively – have for several years officially recognised that regulated firms may, subject to appropriate safe-guards, use electronic or digital means to meet their anti-money laundering / countering the financing of terrorism ("AML/CFT") obligations to identify and verify the identities of their customers. This is in line with the position taken by the Financial Action Task Force ("FATF") – the intergovernmental body whose Recommendations are the accepted international standard on AML / CFT – and followed by many other regulators around the world.

Nevertheless, in our experience (and for reasons touched on in later on in this article) regulated firms in the Channel Islands have in large part continued to rely on traditional, paper-based means of verifying identity, which typically entail customers either producing original identification documentation in face-to-face meetings with their financial services providers, or providing to their financial services providers identification documentation that has been certified in person by a "suitable certifier" such as a lawyer or government official.

However, lockdowns imposed around the world in response to the COVID-19 pandemic have in many cases made it highly impractical or impossible to verify customers' identities by such means, which has brought digital systems for identification and verification of identity ("Digital ID") into focus, and may well accelerate the transition from paper based to digital systems as the default means of verifying identity.

This is a transition that has been actively encouraged by the FATF, which published extensive guidance on Digital ID in March 2020 (the "FATF Guidance", available at www.fatf-gafi.org/publications/documents/digital-identity-guidance.html.), and subsequently suggested "encouraging the use of responsible digital identity and other responsible innovative solutions for identifying customers at on-boarding and while conducting transactions" as a potential policy response to COVID-19 related money laundering and terrorist financing risks. We have already seen similar encouragement from some regulators, including both the GFSC and the JFSC, and expect that others will follow suit.

In what follows, we:

- explain what is meant be "Digital ID";
- take a brief look at the FATF Guidance ;
- take note of the current regulatory positons in Guernsey and Jersey;
- share our perspective on the relatively slow adoption of Digital ID in the Channel Islands; and finally
- offer our views on how Guernsey and Jersey firms should approach the transition to Digital ID.

What is Digital ID?

In the broadest sense, Digital ID encompasses any system that employs digital means to identify and/or verify the identities of subjects, and may range from the use of video calls to review identification documentation where (as during lockdown) in person meetings are impracticable, to sophisticated Digital ID applications, which typically rely on a combination of measures such as geotagging, analysis of biometric information, "liveness testing", and technological safeguards against the provision of manipulated images or forged identification documentation, to verify a subject's identity.

Digital ID systems are not without their particular risks (which vary according to the system in question, but might include, for example, increased vulnerability to cyber-attacks and large-scale identity theft), but also potentially (again, depending on the system) confer significant advantages over traditional methods, including greater security and reliability, the ability to provide "continuous authentication" of identity (i.e. as well as identifying and verifying the identities of customers at the point of take-on), reduced costs and greater efficiency for regulated entities, and greater convenience and a higher level of financial inclusion for customers.

FATF Digital ID Guidance

The FATF Guidance offers "technology neutral" guidance (i.e. guidance that is not tied to any particular technology) to regulators, regulated entities and Digital ID providers on the use of Digital ID, including among other matters a description of a basic Digital ID system, a summary of the benefits and risks of Digital ID for AML/CFT purposes, and guidance on assessing the reliability and independence of a given Digital ID system under a risk based approach to customer due diligence ("CDD").

Although a full analysis of the FATF Guidance is beyond the scope of this article, it is worth outlining its recommendations to regulated entities on the use of Digital ID:

- Understand the basic components of Digital ID systems;
- Take an informed, risk-based approach to relying on Digital ID for CDD, including understanding a chosen system's "assurance levels" (i.e. the degree of assurance that a given Digital ID system provides in identifying and verifying the identity of a subject) and ensuring that those levels are appropriate to the money laundering / terrorist financing risks of the cases in relation to which such system is to be used;
- Consider whether Digital ID systems with lower assurance levels may be sufficient for simplified due diligence in lower risk cases;
- Consider reviewing and revising policies that automatically classify non-face-to-face business as high risk to the extent that Digital ID may be used to reliably identify and verify the identities of customers (although we should caution that any such review should always be subject to any applicable regulatory rules relating to non-face-to-face business);
- Where appropriate, leverage anti-fraud and cyber-security processes to support Digital ID (for example, anti-fraud authentication systems might feed into ongoing monitoring for CDD purposes); and
- Ensure that you have access to, or a process for authorities to obtain, the underlying identification data and supporting evidence.

The Regulatory Positions in Guernsey and Jersey

The rules, regulations and guidance on AML/CFT requirements in Guernsey and Jersey respectively are consolidated in the GFSC's Handbook on Countering Financial Crime and Terrorist Financing (the "GFSC Handbook") and the JFSC's AML/CFT Handbooks for regulated financial services businesses and other sectors (the "JFSC Handbook").

On the whole, the two jurisdictions have taken a similar regulatory approach to Digital ID. In short, both regimes expressly allow for the use of Digital ID (either on its own or together with more traditional methods) to identify and/or verify the identities of customers, and both (like the FATF Guidance) take a technology neutral approach to Digital ID, setting out general principles rather than specific technical requirements relating to its adoption. Both Handbooks also require firms to carry out formal risk assessments in relation to the adoption of any new technology, including Digital ID. The upshot is that the onus is on any firm that wishes to adopt Digital ID to ensure that it understands (and that it has documented its consideration of) how the proposed system works, the level of assurance that it provides and any particular risks associated with it, and to design its controls around identification and verification of identity accordingly.

Otherwise, firms' general obligations around CDD are essentially the same, whether they are met by traditional or digital means (although it is worth keeping in mind that customers identified remotely by digital means may still be considered "non-face-to-face business", which under the JFSC Handbook is subject to additional CDD requirements and under the GFSC Handbook is a risk factor that firms must generally take into account in carrying out their relationship risk assessments.)

Why has adoption of Digital ID been slow in Jersey and Guernsey?

In our experience, the principal issue relates to risk management: underpinning the minutiae of the CDD requirements in both jurisdictions is an obligation on firms to understand the risks of money laundering and terrorist financing presented by their businesses and to manage those risks. Firms in both jurisdictions are also under a specific obligation to risk-assess new products and technologies before they adopt them. Despite the popularity of a handful of trailblazing firms in the high-value offshore financial services market, there is not yet a critical mass of traditional firms using Digital ID technologies to give firms a sense of safety in numbers: while both jurisdictions' regulators have made it clear that they are open to Digital ID in principle, compliance officers and boards remain uncertain of how their regulators will treat any particular technology in practice (particularly if something goes wrong), and might also feel that they do not have the technical expertise to truly understand how the technology works and how to go about risk-assessing it. We have dealt with many firms that are actively considering Digital ID but are wary of being among the first to take it up.

There are no doubt other, related obstacles to the adoption of Digital ID, including lingering uncertainty over the extent to which it is permissible at all. For example, we are aware that there was previously some confusion among firms in Jersey about whether the JFSC Handbook required firms to collect wet-ink certified copies of identification documentation where Digital ID had been used (a situation which would largely have defeated the object of adopting Digital ID in the first place), although the JFSC changed the layout of its Handbook last year to make it clearer that this is not the case.

Furthermore, the up-front commitment (in time and money) involved in risk assessing and implementing a new technology is likely to have discouraged some firms from transitioning to Digital ID while traditional methods remain in widespread use.

Nevertheless, our sense is that Digital ID will quickly become the market standard once a critical mass of early adopters has been reached, a process that may have been accelerated by the recent lockdowns.

How should firms approach the adoption of Digital ID?

We would suggest that, in transitioning to Digital ID, firms take the FATF Guidance, read together with the guidance in the applicable Handbook(s), as the point of departure: the FATF Guidance is the most definitive guidance on the subject currently available, and is likely to inform the approaches of the GFSC and the JFSC (and regulators around the world) going forward.

The most crucial aspect of that guidance, in our view, is around the recommendation that firms take an informed, risk based approach to the adoption of Digital ID, including understanding a chosen system's assurance levels. In our experience, firms often fixate on legal considerations, in particular whether a given system will be permissible from a regulatory point of view. Such considerations are important, but in a sense are secondary to developing a working understanding of how the proposed system works and what level of assurance it provides, because, ultimately, any system that enables a firm to identify and verify the identities of its customers with the same level of assurance as traditional methods (or to a higher level than traditional methods) is likely to be acceptable to the regulator: the deciding factor will be whether the technology is up to the task (and in that regard, it is important to recognise that not all technologies are created equal). As Digital ID becomes more prevalent, we expect that a general understanding of the strengths and weaknesses of various technologies will begin to develop in the market. In the meantime, firms without the necessary in-house expertise may wish to consider engaging third party IT consultants to assist with the technical assessment process.

Once that hurdle has been cleared, firms should approach the adoption of Digital ID in the same way that they would any new system or technology (for example, documenting their risk assessment of the system in question, updating policies and procedures as necessary, engaging with the regulator where applicable, and so on.) If you are considering a transition to Digital ID and are looking for some guidance on the process, please feel free to contact us and we would be happy to assist.

Conclusion

We expect to see continued advancements in this area in the coming years, both technologically and in terms of regulatory approaches, leading to greater certainty and increased standardisation in both respects, and consequently, in all likelihood, the end of paper-based CDD in the foreseeable future.

Contacts

For further information please speak with your usual contact at Walkers or contact:

Jonathan Heaney
Partner, Jersey
T: +44 (0) 1534 700 786
E: jonathan.heaney@walkersglobal.com

Rupert Morris
Partner, Guernsey
T: +44 (0) 1481 748 936
E: rupert.morris@walkersglobal.com

Rachel Amos
Senior Counsel, Jersey
T: +44 (0) 1534 700 720
E: rachel.amos@walkersglobal.com

Tom Fothergill
Senior Associate, Jersey
T: +44 (0) 1534 700 724
E: tom.fothergill@walkersglobal.com

Adam Pickering
Associate, Guernsey
T: +44 (0) 1481 748 915
E: adam.pickering@walkersglobal.com

Joseph Barker-Willis
Associate, Jersey
T: +44 (0) 1534 700 715
E: joseph.barker-willis@walkersglobal.com