Acknowledgements

This survey would not have been possible without the support of the RUSI and ACAMS teams. Special thanks go to project sponsor Lashvinder Kaur, VP Global Strategic Communications, ACAMS, and Jonathan van der Valk at RUSI for their support on this project.

The project team would also like to extend their thanks and appreciation to the many experts who kindly offered their time to review this survey. They were:

- **Dan Stipano** – Partner at Davis Polk & Wardell LLP
- **Anthony Rodriguez, CAMS, CPA** – Chief Global Risk & Compliance Officer and Data Protection Officer at AFEX
- **Sharon Campbell** – Executive General Manager Financial Crime Operations and Transformation at National Australia Bank
- **Calvin Shabazz, Prof. AICB, AICA, CAMS, CFCS, JP** – Principal Consultant and AML Specialist at Bermuda Financial Network, Ltd
- **Atsuo Takada, CAMS** – Senior Systems Analyst at Nomura Research Institute, Ltd
- **Rosalind Lazar** – Regional Anti-Money Laundering Director for ACAMS in APAC
- **Yuji Sato** – Senior Consultant at Nomura Research Institute, Ltd
- **Ken Banks** – Head of Social Purpose at Yoti
- **Julie Dawson** – Director of Regulatory & Policy at Yoti
- **Kate Hotten** – Senior Advisor - VC, Early Stage and RegTech at Fintrail

In addition, special thanks to the ACAMS global membership community of over 81,000 members spread across 175 countries, and its 60 chapters for being part of this landmark initiative.

The opinions expressed in this work are the responsibility of the authors and do not in any way reflect those of RUSI, its directors or its employees. Neither RUSI, nor the authors assume responsibility or liability for the contents of this report, or its reading, use or interpretation. While every effort has been made to verify the data used in this report, no guarantee or warranty is made on its accuracy. You should seek your own professional advice before acting on any of the content in this report.

This report is intended for general guidance and information purposes only and under no circumstances should this report be used as or considered legal or regulatory advice. Each recipient should consult with its legal, business, investments and tax advisors as to the legal, business, investment and tax implications when making any legal, business, financial decision. The information contained in this report is based on survey responses which have been assumed to be reliable. ACAMS, its directors, employees or authors, make no representation or warranty on the responses and such data should be taken “as is”. We do not validate the accuracy, completeness or reliability of the survey responses.
CONTENTS

Introduction —— 4
Key observations —— 6
Methodology —— 7

Section 1: —— 8
General views on Digital ID

Section 2: —— 10
Identifying the role of Digital ID

Section 3: —— 17
Regulations and Digital ID

Section 4: —— 19
Coronavirus and Digital ID
Introduction

The RUSI-ACAMS Global Digital ID Survey provides an insight into how the financial crime compliance community views the utility of Digital ID. It comes at what is a crucial time for the technology. A year after the release of the FATF Guidance on Digital ID and after the Coronavirus pandemic placed a renewed emphasis on its importance, this survey takes stock of how this technology is perceived and the promise it holds for combating financial crime in the future.

As with any survey, it should be recognised that there are certain limitations. Individuals may choose to opt in or opt out of participation and those who participated will reflect that. However, the survey was conducted in collaboration with YouGov, a respected independent research agency who followed the Market Research Society’s code of conduct.

As such, the findings can be taken to offer an illustrative view of industry attitudes to Digital ID, financial crime compliance and risk. The results provide an insight into both the challenges and opportunities of this technology for financial crime compliance. The purpose of conducting this survey is to help shape and inform the policy dialogue on Digital ID and its use by the financial crime compliance community.

Please note, that when this survey refers to ‘Digital ID’, it is specifically referring to what the FATF describes as the: ‘use of electronic means to assert and prove a person’s official identity online (digital) and/or in-person environments at various assurance levels’.

An example of such would be a government-held database of verified identities which financial institutions could access to perform due diligence checks.

Digital ID should not be confused with all technologies used in digital authentication, or the validating of an entity when accessing a service or account. Digital ID can be used in digital authentication, however.

Official identity is defined as the specification of a unique natural person that:

a. is based on characteristics (attributes or identifiers) of the person that establish a person’s uniqueness in the population or a particular context(s), and

b. is recognised by the state for regulatory and other official purposes.

This survey is concerned only with the identification of people and not legal entities. As such, the Legal Entity Identifier is not an example of Digital ID that should be considered for the purpose of this survey.
ACAMS
ACAMS is the largest international membership organisation dedicated to enhancing the knowledge, skills and expertise of AML/CTF, sanctions and other financial crime prevention professionals through training, best practices and professional development. ACAMS is present in over 175 countries and regularly works with global think-tanks and other like-minded organisations in the quest to end financial crime.

RUSI
RUSI is an independent defence and security think-tank based in the United Kingdom. RUSI’s Centre for Financial Crime and Security Studies has conducted a wide array of research on the impact of new technology on financial crime and compliance. To read more about RUSI’s work visit www.rusi.org/CFCS.

YouGov
RUSI and ACAMS partnered with YouGov to deliver this survey.

About the Authors
Isabella Chase, Research Fellow, Centre for Financial Crime and Security Studies, RUSI.
Rick McDonell, Executive Director, ACAMS and Former Executive Secretary of FATF.
Key observations

In general, respondents indicate that there is a fairly good understanding of what Digital ID is in the financial crime community. 82% of respondents were at least familiar with the concept of Digital ID and what it can be used for. Understanding was highest in the private sector, where 43% of respondents said they had a good understanding of Digital ID. Geographically, respondents in Asia and Oceania had the best understanding of Digital ID.

Overall, 86% of respondents view Digital ID as a positive innovation, with the private sector being the most convinced of this.

When asked who they would trust to make a Digital ID respondents overwhelmingly said they would trust government issued Digital IDs, with 87% of respondents saying they would do so.

The survey asked respondents, if they were not currently able to use Digital IDs for financial crime compliance, would they like to do so. 76% of respondents would like to. When asked what is stopping them from using Digital IDs in this way the most commonly stated barriers were a lack of standardisation across the globe, followed by a lack of guidance and cybersecurity concerns.

85% of respondents think that Digital ID would benefit customer onboarding. In countries where Digital ID is not currently in use for onboarding, 65% think it would make onboarding more effective and 67% think it would lower the cost of onboarding. In countries that already use Digital ID for customer onboarding, 44% think that it has made onboarding more effective and 48% think it has lowered the cost of this process.

Two-fifths of respondents believe that the gains made by using Digital ID in the fight against financial crime will be evenly split between increasing effectiveness of controls and the efficiency of compliance.

In general, respondents believe that the greatest risks of Digital IDs come from fraud and the exploitation of the vulnerable. Despite these perceived risks it was felt by respondents that paper-based IDs are still more vulnerable than Digital IDs.

Respondents were split on whether their local data protection legislation enabled the use of Digital ID for financial crime compliance. Respondents in the Middle East (69% yes) and Africa (68%) most strongly agree that their legislation enables the use of Digital ID, whereas respondents in South America (27% no) agree that it does not.

Over half of respondents say that the pandemic has made them more accepting of Digital IDs in general and a slightly lower proportion say it has made them more accepting of the usefulness of Digital IDs for financial crime compliance. This may come as a surprise for those who think the pandemic has made people more accepting of new technology. The increase in fraud over the past year, however, may explain this, as fraud risk is perceived to increase with the use of Digital ID.
Methodology

The survey was distributed to ACAMS members and the members of RUSI’s Centre for Financial Crime and Security Studies’ mailing list. It was also sent directly to stakeholders in the Digital ID community. This report is based on 304 responses received between January 14 - March 5, 2021.

In total the survey received responses from respondents based in 70 different countries, with the highest responses from the US, UK, India, Canada and Australia. Where it is relevant, this report states where there were significant regional differences in how respondents answered the survey.

The countries with the most respondents were:

- **US**: 63
- **UK**: 55
- **India**: 10
- **Canada**: 9
- **Australia**: 9

The survey asked respondents to identify which sectors they work in. 74% of respondents said that they work in the private sector, 15% say they work in public sector with the remaining 11% working in the third sector, which includes academics, charities, NGOs and think-tanks. Out of the 74% that work in the private sector, 47% work in traditional financial institutions (of which 38% work in international banks), 21% in FinTechs, 11% at technology providers and 20% in the non-financial sector.

When asked if they have a good understanding of Digital ID and what it can be used for, 82% indicated that they are at least familiar with Digital ID, with 41% stating that they have a good understanding of what Digital ID is. 14% of the total said that they had heard the term Digital ID but were not confident in their understanding of it.

Understanding is highest in the private sector, with 43% of private sector respondents saying that they have a good understanding of Digital ID. This figure reduces to 33% in the public sector and 35% in the third sector.

Geographically, respondents in Asia and Oceania have the best understanding of Digital ID, with 54% of respondents in Asia saying they have a good understanding and 53% in Oceania.
To establish the level of familiarity that respondents have with Digital ID the survey began by asking respondents some general questions about how they perceive Digital ID. The survey asked if respondents had ever used a Digital ID, with 47% saying that they had used a Digital ID before, and 51% of those had used a Digital ID to gain access to a financial service or another service that falls under the AML/CFT regime. 53% of respondents said that they had not used a Digital ID before.

Respondents who had said they did not have a good understanding of Digital ID were asked what areas of Digital ID they needed further clarification on. The most common areas included: privacy concerns, use cases, insufficient regulatory guidelines and the need for international best practices.

Despite these concerns, when asked if they view Digital ID as a positive innovation, 86% of respondents said they did, with the private sector being the most convinced of this.
Section 1: General views on Digital ID continued

Respondents were asked to consider, based on the jurisdiction in which they reside, who they would trust to issue Digital IDs. At present, Digital IDs are issued by a variety of stakeholders around the world. They can be issued by governments, private companies, charities or as collaborations between various stakeholders. Overwhelmingly, it was felt that respondents could trust government-issued IDs with 87% of respondents saying they would trust a government-issued Digital ID.

The least trusted Digital IDs were those issued by NGOs with 49% of respondents saying they would not trust a Digital ID produced by an NGO. It is worth remembering however, that NGOs tend to only create Digital IDs for a limited number of use cases such as for refugees or displaced people.

When looking across the regions, Oceania and Asia are the most trusting of government-issued Digital IDs, with 100% and 93% of respondents respectively saying they would trust them.
Section 2:
Identifying the role of Digital ID in the fight against financial crime

Digital IDs can have various roles in the fight against financial crime. To help identify where this technology could make the greatest gains respondents were asked how they perceive the impacts it could have on the efficiency of compliance practices and the effectiveness of financial crime controls. They were also asked whether Digital IDs could create new financial crime risks and whether Digital IDs are likely to have an impact on financial inclusion.

Over half of respondents are aware of Digital IDs being used for financial crime compliance in their country. The highest proportion can be seen in the Middle East, with 82% of respondents in that region having awareness that Digital IDs are being used in this way. The lowest use was in South America, with 23% of respondents being aware that Digital IDs are used. In Europe 51% of respondents were aware of Digital ID being used for financial crime compliance, with 44% being aware in North America.

---

**Q5. Are you aware of Digital IDs being used for financial crime compliance in the country you reside in?**

*Base: All respondents (304); Private sector (225), Public sector (45), Third sector/Other (34). Respondents in N.America (93), S.America (11), Europe (98), Africa (22), Asia (46), Middle East (17), Oceania (17)*
The survey asked respondents if they were not currently able to use Digital IDs for financial crime compliance would they like to do so. 76% of respondents who do not currently use Digital ID for financial crime compliance would like to. When asked what is stopping them from using Digital IDs in this way the most commonly stated barriers were a lack of standardisation, followed by a lack of guidance and cyber security concerns.

The survey asked respondents whether in the face of these challenges their organisations would have the capacity to implement Digital IDs into their systems. At total level, around three-fifths believe their organisation has the capacity to implement Digital IDs. Those in the private sector are most confident, but those in the third sector are more likely to say their organisation could not implement a Digital ID solution.
How could Digital ID be used in financial crime compliance?

Financial crime compliance is a multi-step process that must be reviewed on a rolling basis. The survey asked respondents where in this process they thought Digital IDs would have the greatest impact and what difference this would make to their compliance procedures.

When asked where in the compliance lifecycle Digital IDs would be the most useful respondents agreed that customer onboarding would be where Digital ID would be the most useful, with 85% giving this response.

The survey asked respondents to state why they think the customer onboarding would see the greatest benefits. Around three-quarters of respondents said that Digital IDs will help overcome labour intensive manual checks to verify identity. And when pressed to select just one benefit, streamlining onboarding was the most commonly cited benefit. Of note, only 66% of respondents thought that Digital IDs would overcome a lack of documentation.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labour intensive manual checks to verify and authenticate identity</td>
<td>74%</td>
</tr>
<tr>
<td>The use of forged documents and/or the fraudulent use of another person’s identity</td>
<td>71%</td>
</tr>
<tr>
<td>Digital ID will streamline onboarding for the customer, reducing friction, churn and cost</td>
<td>67%</td>
</tr>
<tr>
<td>Lack of necessary documents for identification and verification, including expired documents on file</td>
<td>66%</td>
</tr>
<tr>
<td>Human error</td>
<td>65%</td>
</tr>
<tr>
<td>Inability to conduct onboarding checks in person</td>
<td>63%</td>
</tr>
<tr>
<td>Lack of confidence in ID checks performed by third parties</td>
<td>56%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
<tr>
<td>None of the above</td>
<td>4%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>6%</td>
</tr>
</tbody>
</table>

Q8. When considering customer onboarding, which, if any, of the following common problems do you believe Digital ID can help overcome? Please select all that apply. Q8_single. And which common problem do you believe Digital ID can best help overcome? Please select one. Base: All respondents (304)
How could Digital ID be used in financial crime compliance? continued

And which common problem do you believe Digital ID can best help overcome?

Digital ID will streamline onboarding for the customer, reducing friction, churn and cost 22%
The use of forged documents and/or the fraudulent use of another person’s identity 21%
Labour intensive manual checks to verify and authenticate identity 18%
Inability to conduct onboarding checks in person 9%
Lack of necessary documents for identification and verification, including expired documents on file 8%
Human error 6%
Lack of confidence in ID checks performed by third parties 5%
Other 1%
None of the above 4%
Don’t know 6%

Q8. When considering customer onboarding, which, if any, of the following common problems do you believe Digital ID can help overcome? Please select all that apply. Q8_single. And which common problem do you believe Digital ID can best help overcome? Please select one

Respondents were asked if they currently use Digital ID for customer onboarding and whether this has impacted the effectiveness and cost of this process.

Two-thirds of respondents who do not currently use Digital ID for onboarding believe that the use of Digital ID would increase the effectiveness of onboarding, the highest proportion of which are in South America. Conversely, in countries where Digital ID is already in use for onboarding only 44% of respondents say that Digital ID has increased the efficiency of onboarding, although a quarter said that they didn’t know.

Similarly, in jurisdictions not currently using Digital ID for onboarding, 67% think it will lower the cost of this process whereas in jurisdictions already using Digital ID only 48% think it has lowered the cost, although 27% say they were not sure. It appears that expectations for how Digital ID could benefit onboarding are not always met.

When looking at the remaining stages of the compliance lifecycle, 76% of respondents thought that Digital ID would be useful for client exiting. Followed by payment screening, ongoing monitoring and transaction monitoring. For transaction monitoring the main benefit was perceived to be that respondents will have ongoing assurance that their customers are who they say they are (56%).

Three-fifths of respondents are confident a balance can be achieved between the customer’s experience of the identity verification process, and requirements for compliance, privacy, and security being fulfilled. Just a tenth are not.

Q4. To what extent, if at all, do you agree or disagree with the following statement? “In general, I view Digital ID as a positive innovation”. Base: All respondents (304); Private sector (45)
This survey wanted to find out if respondents had considered the benefits of Digital ID outside of financial crime compliance and in addition to this, if they thought that Digital IDs would impact financial crimes themselves. The survey asked if Digital IDs could impact the prevention, detection or disruption of financial crimes.

When thinking about the prevention of financial crime, the biggest anticipated impact of Digital ID is in the provision of consistent customer ID information. This “golden source” of customer ID was seen by 62% of respondents as the most important gain in the prevention of financial crime. In addition, 57% thought that Digital ID would improve the analysis of data to better inform red flags and known typologies.

When thinking about detecting financial crime, the biggest expected impacts are in detecting hidden network relationships and in being able to use Digital IDs in conjunction with other data points such as geolocation data to detect suspicious behaviour.

When asked about how Digital IDs could disrupt financial crimes, 67% of respondents think that Digital IDs could allow for more consistent information sharing between regulated entities and law enforcement. This is complemented by the finding that 65% of respondents believing that Digital IDs would improve the quality of identity matching in analysis of bulk SARs data by FIUs.

Respondents were asked, when considering the use of Digital ID in the fight against financial crime, do they think the greatest gains will be made in the efficiency of the compliance process or in the effectiveness of the financial crime controls at combating crime. Two-fifths of respondents believe that gains will be evenly split between effectiveness and efficiency. Respondents in Asia and Oceania are more likely to think the gains will be in efficiency.
This survey has shown that Digital IDs are perceived to be beneficial for the fight against financial crime and will aid in both the efficiency of compliance and the effectiveness of controls. Digital IDs, however, are not fool-proof technologies and present risks to the user and to the institutions that accept them. This survey asked respondents if they had considered the risks of Digital IDs. In general, respondents perceive the greatest risks of Digital IDs to come from fraud, cyber security and the exploitation of the vulnerable. Despite these perceived risks it was felt by respondents that paper-based IDs are still more vulnerable than Digital IDs.

Almost half of respondents say they are concerned that Digital ID could create new financial crime risks, with concern highest among respondents in Asia and Africa. Respondents in Europe were the least concerned about the creation of new financial crime risks.

Respondents were asked to select the risks that they are the most concerned about. On average most respondents were concerned by data breaches and the exploitation of the vulnerable. 71% of the private sector were concerned by the risk of data breaches in comparison to 49% of the public sector.

In addition to the direct risks posed by Digital IDs for financial crime, respondents were also asked if they are concerned about risks that relate to Digital IDs. Here, 70% of respondents were most concerned by inadequate technology and controls to maintain and regularly update the records of a Digital ID and 63% of respondents were concerned about individuals selling their Digital ID credentials to organised crime groups.

The risks posed by Digital IDs should be put into context and compared with those posed by paper-based IDs. Respondents were asked which they perceive to be more vulnerable to exploitation by criminals. In general respondents believe a paper-based ID is more vulnerable than a Digital ID, although a third think they are equally vulnerable.
Effective financial crime compliance systems minimise unintended consequences, such as financial exclusion. Financial exclusion can occur when individuals do not have the necessary documentation required to pass ID and verification checks as part of financial crime compliance. Digital IDs can help individuals overcome this challenge by allowing them to create an identity without traditional documents or to “build” an ID progressively over time. This survey asked respondents if they thought Digital IDs would have an impact on financial inclusion.

Respondents tended to agree that Digital ID will make it easier to offer financial services to a wider array of customers, with 45% thinking that it will become easier and 23% taking a neutral stance.

Those that say it will make offering financial services easier say so because their organisation would have better knowledge of who they are dealing with (67%). In addition, 55% think that Digital IDs would make them more confident offering products which utilise a risk-based approach and factors such as simplified due diligence.

For those that say it will make offering financial services harder think so because they will still need greater clarification from regulators on offering simplified products (41%) and because the cost of compliance will still be too high to offer products and services to the financially excluded (41%).

When asked if they were concerned that Digital IDs might drive financial exclusion, approximately a third of respondents say they are concerned that it could drive financial exclusion, although 28% are not.

Respondents were given the opportunity to expand on whether they are concerned if Digital ID will drive financial exclusion, the full list of responses can be found in the appendix. In summary, respondents were concerned that the financial inclusion hurdles that already exist today will be perpetuated by Digital ID instead of being overcome. They were also concerned that certain groups will be left behind by the digital divide.
Section 3: Regulations and Digital ID

Digital IDs exist in complex regulatory environments which must balance financial crime requirements with concerns over privacy. To better understand this balance this survey asked respondents if they were up to date with the latest guidance on the use of Digital ID in financial crimes compliance and whether data privacy legislation enables their use of this technology.

FATF Guidance

In March 2020, the Financial Action Taskforce (FATF), the international standard setting body for financial crime controls, issued guidance for the use of Digital ID in financial crime compliance. The guidance is designed to assist entities who wish to use Digital ID to identify their customers with a high level of assurance.

Around a quarter of respondents have read the FATF Guidance on Digital ID, with a further two-fifths saying they are aware of it and 32% saying they were not aware of the guidance.

Respondents in the public sector are least likely to have read the FATF Guidance, whereas those in the third sector are the most likely to have read it.

Of those who have read the guidance, 63% believe that it gives enough detail to understand what to look for in a reliable Digital ID scheme. 54% believe that it gives sufficient guidance on how to use Digital IDs for remote account opening.

Have you read the March 2020 FATF Guidance on Digital ID?

In your opinion, does the FATF Guidance on Digital ID give you enough detail to understand what to look for in a reliable Digital ID scheme?

In your opinion, is the guidance on the use of Digital ID for remote account opening sufficient for you to use Digital ID for this purpose?

Base: All respondents (304)
Data privacy

Data privacy and protection is a key concern for many when considering the utility of Digital ID in financial crime compliance. Respondents were split on whether their local data protection legislation enabled the use of Digital ID for financial crime compliance. Respondents in the Middle East (69% yes) and Africa (68%) most strongly agree that their legislation enables the use of Digital ID, whereas respondents in South America (27% no) agree that it does not.

For those who do not have data privacy legislation in place, 43% think this makes it more difficult to use Digital ID in financial crime compliance.

71% of respondents think that Digital IDs should be portable, meaning that they can be used across products, services and potentially across borders.
Section 4: The Coronavirus pandemic and Digital ID

The Coronavirus pandemic has sparked new urgency in the conversation on Digital ID. With customers told to stay at home but still needing to access finance, Digital ID was posited as the solution to verifying identity during the pandemic.

Survey respondents, however, were not universally convinced, with just over half saying that the Coronavirus pandemic has made them more accepting of Digital ID in general and slightly less saying it has made them more accepting of the usefulness of Digital IDs for financial crime compliance.

It is possible that respondents remain unconvinced due to the perceived risks of Digital ID, such as fraud, which have intensified during the pandemic.

<table>
<thead>
<tr>
<th></th>
<th>Private sector</th>
<th>Public sector</th>
<th>Third sector/Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usefulness of Digital IDs for financial crime compliance</td>
<td>49%</td>
<td>28%</td>
<td>7%</td>
</tr>
<tr>
<td>Digital IDs in general</td>
<td>54%</td>
<td>27%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Q31. What effect, if any, has the coronavirus pandemic had on the extent to which you accept...

Base: All respondents (304)