Visa Response to the European Commission White Paper on Artificial Intelligence

June 2020

About Visa

Visa welcomes the opportunity to respond to the European Commission's Artificial Intelligence White Paper. Our mission is to connect the world through the most innovative, reliable, and secure payments network – enabling individuals, businesses, and economies to thrive. Visa's relentless focus on innovation is a catalyst for the rapid growth of connected commerce on any device, a driving force for increased digital acceptance, and a cornerstone of safety and security across the digital economy.

Visa currently facilitates commerce across more than 200 countries and territories. As a leading global payments technology company, Visa understands what it means to function, innovate, and invest in a continuously evolving and interconnected digital world. The global nature of our business also gives us a holistic perspective on regulation, which is particularly useful when considering regulatory approaches to 'borderless' markets and technologies, such as data and artificial intelligence ('AI').

Our 'north star' for data use (including data-driven technologies such as AI) is that it should first, and foremost, benefit individuals, businesses, and economies. This overarching approach is underpinned by our commitment to those who use our products and services that we will be accountable stewards of their data, will uphold their privacy, and will promote high standards of responsible, ethical practice in every market in which we operate.

Visa pioneered the use of AI in payments in 1993, becoming the first payments network to use neural networks for real-time, risk-based fraud analytics. Visa Advanced Authorisation ('VAA') now prevents approximately USD 25 billion of fraud annually. Today, we are increasingly leveraging the power of data and data-driven technologies, such as AI, for a wide variety of purposes across our business, including security, product and service delivery, operational efficiency, and network reliability. We are confident the next generation of payments experiences (such as 'conversational payments', behavioural biometrics, and automation of bespoke 'point of sale' shopping experiences) will be powered by AI.

1. The potential for AI in Europe

As per Visa's response to the European Commission's Data Strategy consultation, we support the Commission's vision to create a human-centric and trustworthy digital environment in Europe for the use of data and data-driven technologies, such as AI. Visa is also aligned with the Commission's aim to create a common regulatory framework in Europe, and we are encouraged by the White Paper's measured approach to regulating AI.

With its world-leading privacy and security regimes, and its proposals for a Single Market for Data, Europe is a potentially rich environment for the development and use of AI. From start-ups to large scale enterprises, this usage is expanding, as is innovation, research, and development. The pace of this activity, and the opportunity cost inherent in an overly stringent approach to AI, requires regulation that is sufficiently agile to adapt to change. The Commission is correct in identifying potential harms that result not only from the use of AI, but also from unduly limiting its use, which would risk Europe missing many advantages in terms of socio-economic progress and international competitiveness. We welcome the White Paper's acknowledgement of this, and of the principle that new regulation should therefore be a response to clearly identified problems, for which practical solutions exist (this is discussed further below).

Visa is optimistic about the opportunity for AI in our sector (and beyond) to power economic growth and positive societal transformation. Innovation in AI, particularly the ability to build fair, accurate, fit-for-purpose models, depends on access to large, diverse data sets that can flow across borders and sectors. We believe the Commission's "European Strategy for Data" (designed to incentivize and facilitate a data-sharing ecosystem across the bloc) is therefore, a potentially powerful catalyst for the development of AI in Europe, as this can achieve across the EU what would be much more limited at the state-level. Similarly, the Commission's proposals for EU-level action (such as funding programmes, research and development, skills, and talent programmes) through a Coordinated Plan all leverage the potential of combined action to drive investment, innovation, and regional competitiveness.

Europe has a strong history and institutional culture of public-private partnerships to develop and advance policy objectives. This collaboration is critical to support necessary synergies and to share the estimated cost of the digital transition, and it is positive that the Commission envisages this path forward for AI. Visa looks forward to continuing and expanding our numerous partnerships with national and local governments, universities, research and innovation centres. Visa's Innovation

Centre and two Data Science Labs based in Europe are all ramping up activity, including in AI, and in support of local start-ups and FinTechs.

The ability to leverage local talent is extremely important, and Visa welcomes the Commission's objective to establish and support skills programmes for AI. Much more will need to be accomplished in this area for Europe to achieve the EU's goal of international competitiveness in AI. Industry has a role to play in promoting new skills, sharing knowledge, resources and best practices. However, to foster a world-class employment market for AI in Europe, education and skills policy must continue to increase its focus on technology. A further joint aim is that of improving the critical diversity required in AI development to avoid bias. This is achieved by including a diversity of backgrounds, perspectives, and experiences in the AI community – a far cry from where the industry stands today. This will be to the benefit of businesses, citizens, and society as a whole and represents an area of rich potential for public-private collaboration.

2. Building trust in AI

The public relationship with new technologies is often challenging, as accelerated technology development and penetration outpaces the usual depth of public understanding. This has been further marred in the case of data, for example by high-profile spotlight cases of data breaches and privacy abuses, exacerbating consumer's existing mistrust of data use 1. Historic suspicion of AI's future role in society (driven by popular culture) is being replaced with less sensationalist and futuristic, but more immediate and tangible, concerns over issues such as privacy, fairness, and inclusion. As uses of machine learning and AI expand, public awareness of not just the positive, but also the potentially negative outcomes, are becoming more widely publicised and understood by the general public. A current high-profile example is the potential for racial bias in facial recognition AI.

Public perception is certainly not all negative and, in some contexts, the use of algorithmic technologies has focused the attention of consumers in a positive sense. Voice assistants, chat bots, smart-thermostats and doorbells, matchmakers, and music recommendation engines, for example, have all served to embed an understanding of and familiarity with algorithms in the minds of the public2. However, it is clear there is much more to be done if automated decision-making is to reach its full potential.

The ecosystem of trust required to earn the public mandate for the uptake and usage of new digital technologies at scale can only be created through collaboration between industry and policymakers. This will require a balanced approach, by building public confidence in new technologies, whilst

supporting innovation and global competitiveness (see below). Consumers cannot be expected to have the necessary technical understanding of algorithms that is currently needed to feel empowered and informed in decisions about their data. Instead, public and private stakeholders must work to build public trust and confidence in the humans behind the AI, including the AI development and research community, firms using AI, and the regulators governing them. This will primarily be based on open, honest communication and an underlying framework of ethical principles and responsible practices.

Effective public communication

It is useful, when considering effective public engagement strategies concerning AI, to keep in mind that "the public" is not a single entity. A global consumer attitudes study3 conducted for Visa in 2019 found at least five distinct personality segments (based on different levels of technical engagement and sophistication), with large variances in attitudes and behaviour relating to data and AI. We are continuing to build on this research, but findings suggest these divergences will only be more pronounced with more complex AI, and different approaches will be required to reassure and incentivize each consumer group. This will require a combination of public and private sector research and communications strategies.

Trust from consumers is hard earned and public mistrust in new technologies is likely to continue in the short to mid-term. Therefore, over and above improving public awareness and familiarity with AI, trust in this area must be built by consumers consistently experiencing outcomes which uphold their fundamental rights, which are fair, and which deliver value of some kind to them. These outcomes must also be explainable with logic that they can understand. In short, telling consumers to trust AI is one thing; showing that the use of AI is trustworthy is another. This is elaborated on further below.

3. The role of ethics in trustworthy AI

Transparency is one helpful tool to demonstrate trustworthiness as described above, but only to the extent it demystifies, rather than increases complexity. For example, ensuring consumers are aware they are dealing with AI, not a human, is helpful; presenting consumers with reams of source code is not. It is therefore critical to design AI to be explainable. Not in such a way as to expose commercial secrets, nor to limit accuracy beyond a reasonable degree; rather to ensure the core components of a responsible, ethical approach are clear, for example being able to explain data integrity, accountability structures, how bias was mitigated, and the rationale behind the model. The aim should

always be to ensure a consumer understands why a decision was made, and what they can do about it.

As demonstrated above, there will often be a need to consider how best to balance important ethical aspects of trustworthy AI, such as transparency, explainability and accuracy (amongst others such as privacy and security). Many of these concepts could be described as falling under the heading of 'AI ethics', a field which is rapidly advancing due to work of stakeholders across academia, industry and policy. The Commission's establishment of the High-Level Expert Group ('HLEG'), for example, has demonstrated the positive impact of public-private collaboration in this area. The core principles established by the HLEG 'Ethics Guidelines for Trustworthy AI' (in which Visa has been a stakeholder and pilot process participant) have helped to drive consistency of understanding and approach, anchored on shared common values like trust, fairness, explainability, effectiveness, safety, and human oversight.

However, it was clear through the debate and discussion, which characterised the development process of the 'Ethics Guidelines for Trustworthy AI' (and similar initiatives in which Visa has participated), that the ethical constructs which underpin this field are inherently fluid, often contextual, and cannot necessarily be translated directly into law. This is consistent with the conventional application of ethics as a discipline that exists in tandem with legal requirements or takes over where the law ends, rather than a concrete approach which can be translated into prescriptive rules. This in turn indicates that ethics should inform, not define, regulatory approaches.

It is in the interests of industry participants seeking to drive the uptake of AI to work individually and collaboratively on these ethical frameworks - to mitigate risk, protect trust and advance best practice for the practical application of ethics in different sectors and varieties of organisation. As a globally trusted brand, Visa has consistently committed to strong internal governance that goes beyond legal compliance – this is reflected in our approach to AI.

4. Definition of AI

New regulatory frameworks must deliver an appropriate degree of legal certainty over what applications will fall under the new rules. However, an overarching legal definition of AI constitutes an ongoing challenge for academia and policymakers, with a significant diversity of views, in particular around how broad or narrow this definition should be. It is important for legal certainty that some

definition be provided. The long-running debate around this issue, however, is indicative of the complexity of attempting to define AI.

The definition proposed by the HLEG is an example of a broad conceptualisation of AI. General definitions present issues in several regards. The general principle behind broad definitions is to 'future proof' against technology evolution. This is certainly important, however given the very large number of proposed interpretations of AI (past, present and future), a definition broad enough to accommodate all of these risks becoming ineffective. A more tailored definition is therefore more useful, so long as the regulation allows flexibility and agility for the definition to evolve along with the technology.

There exists already today extensive, long-running use of many well-established modelling techniques for a multitude of purposes. Overly broad definitions risk encompassing such a wide range of use cases as to result in regulation of impractical scope, as well as cases where regulation is inefficient, ineffective, or unsuitable. This would pose a significant disincentive to innovation and investment. Moreover, many less complex, already widely used models do not present the same risks or harms as cutting-edge AI systems, which may require greater scrutiny and governance. It is therefore necessary for industry and policymakers to work together to determine which techniques are characterised by a degree of complexity, or other distinguishing technical feature, that merits increased governance. Traditional software and systems, incorporating hard-coded predictable rules, is very different to cutting-edge AI designed to operate and react like humans by ingesting data and adapting its learnings with an increasing degree of autonomy.

Sectoral regulatory guidance

We appreciate the Commission's statement that flexibility is required in an overarching definition to cater for technology evolution. However, as explained above, it is extremely important that the definition of AI is not reduced to all instances of data and algorithms used for predictive modelling. We would therefore suggest a narrower definition be used in overarching legislation, and additional sectoral regulatory guidance (which is more agile than primary legislation) be used to define a clear subcategory of AI systems, in line with international and industry standards. This could include specific systems where factors such as opacity, complexity or degree of autonomy indicate a level of sophistication or risk requiring additional governance. If the basis is to be formed from the HLEG definition, we would propose removing language around hardware, which cannot itself behave intelligently. Importantly, the definition should be specific that the systems it intends to cover are those which are taught or learn from experience, thus avoiding the undesirable consequences described above of including all traditional rule-based AI.

5. Regulatory approach

We welcome the Commission's dual strategy (described in the White Paper as 'an ecosystem of excellence' and an 'ecosystem of trust') to incentivise AI development, whilst at the same time ensuring measures are in place to drive responsible practices that uphold fundamental rights. Any new regulatory frameworks should maintain a strong focus on both aims, recognising that they are complementary and not mutually exclusive. Greater use of responsible AI will drive trust, trust will drive uptake, and so on. Governance should therefore be designed to foster an innovative and trustworthy ecosystem for EU AI, which addresses regulatory gaps effectively, without producing a chilling effect on the overall advancement of AI in Europe and the benefits it can deliver.

The overall approach laid out by the Commission appears proportional and balanced. We are reassured by the principle of avoiding over-prescriptive regulation which would place the EU at a competitive disadvantage in the development and innovation of AI.

Outcome-based regulatory approach

As discussed above, public trust is built through consistent positive consumer experience of the use of AI driving outcomes that uphold fundamental rights and deliver benefits. Visa therefore believes that maintaining a focus on outcomes will incentivise companies to place impact on consumers at the heart of their approaches to AI, rather than setting the bar at compliance with legal process. This does not detract from the importance of process. Indeed, well-designed outcomes-based frameworks are capable of driving proper risk management, accountability and ethical considerations, whilst allowing companies to operate flexibly and efficiently, keeping pace with evolving technology and community best practices. The sheer diversity of the organisations developing and using AI requires a degree of flexibility to accommodate different approaches; however, delivery of positive outcomes is a universally applicable standard. Industry and regulators will need to work together to define the principles and objectives of such an outcomes-based approach.

Consider existing regulation

As discussed in the White Paper, developers and deployers of AI are already subject to a wide body of EU legislation on fundamental rights, consumer protection, unfair commercial practices, competition law, and product and safety liability. Our own sector of financial services, and, within this, payments, is highly scrutinised and regulated, both at national and supranational levels. We agree

with the Commission that much of the existing legislation (in the areas listed above and others) can be applied or adapted to apply to AI. We understand that this approach would be the most efficient route to effective outcomes in many cases, supporting European competitiveness by avoiding the imposition of undue regulatory burden for businesses investing and innovating in Europe. We believe this route is likely to be sufficient to address many potential harms. A holistic review of sectoral regulation should be undertaken for this purpose, as a pre-requisite to the introduction of any new rules. This will require consultation with industry, and close co-ordination between vertical and horizontal regulators to ensure consistency of approaches and avoid unnecessary cumulative or duplicative regulation. As part of this process, and in recognition of the diversity of sectoral and organisational approaches, the potential role of industry-led standards and codes of conduct should be closely examined. These can be more flexible and agile than regulation, whilst also effective in driving best practice and clarifying what practical application of a regulation might mean for a given sector4.

Alignment and coordination with existing sectoral regulation and industry standards

This co-ordination around regulations and standards impacting AI will continue to be of great importance going forward, particularly in the area of compliance and enforcement (see below). We recognise that regulators will have context-specific approaches, as is appropriate. However, close attention will be required to ensure streamlining both of existing and new regulation, as well as between AI-specific and other areas of law. It is of some concern to Visa today that this degree of co-ordination amongst regulators, even at the national level, is not always the case in areas touching on data and AI. For example, we have observed instances where privacy regulation and sector regulation have moved in opposite directions or appeared to contradict. This is clearly a complex evolving area of policy, but we would emphasise that this is unhelpful to investors seeking legal certainty.

Collaboration and co-ordination are equally important at the supranational level, as described above in reference to the need for cross-border interoperability and alignment to the greatest extent possible. We agree with the proposal to establish a permanent network of national competent authorities in various sectors to complement existing expertise, share best practices and develop a harmonized approach to conformity assessments and oversight of AI applications and services. We encourage the Commission to play an active role in ensuring this cross-sector regulatory engagement and alignment is achieved.

6. International alignment and interoperability of an EU AI framework

As a global corporate citizen and a trusted heritage brand, we agree with the emphasis placed by the EU on high standards of consumer protection and respect for fundamental rights. The Commission's commitment to building and strengthening international alliances around these issues (in and outside of the EU) is commendable. We see global advocacy and diplomacy, as well as the mechanism of international trade agreements, as key tools to achieve this.

These relationships of course help to promote political and regulatory alignment across borders, which is critical in the era of digital commerce. In a global, interconnected economy, too great a degree of divergence poses real risks to the socio-economic benefits and opportunities of data use. As discussed above, this is especially the case for data-driven technologies such as AI, where data flow and interoperability is essential to achieving the diversity and data quality required to build responsibly. As a global business, we vastly prefer cross-border regulatory agreements and alignment to a patchwork of local rules. We are also strongly opposed to data localisation, and due recognition should be given to the leading role the European Commission has played in advocating against such policies, which damage economic growth and result in harming the communities it seeks to protect.

To be effective, any new regulation must therefore be streamlined, cross-border, and supportive of trusted data flows. We are reassured by the Commission's commitment to creating this consistency and certainty across the EU. The GDPR has proved successful in this regard, driving up standards of consumer privacy and contributing to the focus on consumer welfare at the heart of many evolving approaches to data use, not just in the EU but also around the world. The GDPR also delivers the substantial benefits of the streamlined cross-border regulatory approach described above. Importantly, the framework also affords national jurisdictions the opportunity and respect to pursue their own approaches to achieving equivalence in mechanisms selected for data-sharing (for example by pursuing adequacy decisions). Allowing countries to maintain flexibility in that regard has proved to be a highly effective model for reconciling international and domestic approaches, thus enabling cross-border data flows without violating the data sovereignty of individual jurisdictions. We hope new regulatory frameworks for AI will follow the same principle. Similarly, industry standards (as discussed in Section 5) can be extremely helpful in driving best practice and clarity of regulation in practice. This is equally true at the international level, where international standards bodies such as the International Organization for Standardization (ISO) continue to help drive consistent and globally interoperable standards within the industry.

7. Risk-based and outcomes-based regulatory approaches

As referenced above, Visa agrees that risk should be a critical delineator for regulators in defining the scope of new regulation and that high-risk applications merit a higher degree of scrutiny than low-risk use cases. We believe the proposals in the White Paper go some way toward establishing a sensible approach in this respect; however, we would urge caution in several respects.

Assigning risk

Firstly, a risk-based approach depends on risk being attributed in an accurate, effective manner to the various use cases. The Commission's current proposal is for a cumulative two-tiered approach based on: a) identified high-risk sectors; and b) an application of AI in which significant risks are likely to arise. This will certainly be helpful to ensure new regulation is targeted toward sectors and use cases where it is most required. However, a model which is technically capable of causing significant harm may be highly likely to do so in one use case, and almost entirely unlikely to do so in another. As a result, the two-stage test on its own may lead to an overly broad spectrum of cases that qualify as high-risk.

Visa's AI Model Risk Management ('MRM') process includes a similar multi-layered process of risk assessment, the basis of which is a matrix of 'potential seriousness of harm versus likelihood of harm in this use case'. We have deliberately separated seriousness from likelihood, as likelihood often involves its own risk analysis based on the specific context in which this model is being applied. Separating the criteria in this way helps us to apply a proportionate, targeted approach, ensuring risk is mitigated where this is most needed. The White Paper goes some way toward this, including as its second criteria: "AI used in such a manner that significant risks are likely to occur". However, to address the issues above, Visa would suggest 'likelihood' be made explicit as a third discrete criteria to be evaluated separately from the severity of harm. The three criteria would thus be: a) sector; b) significance or severity; c) likelihood of risk. It should be noted that there are several categories of risk used by risk professionals and it will be significantly easier for both companies are regulators if there is alignment between new legal language and established industry terminology.

High-risk applications

Secondly, we are concerned that too broad a categorisation of high-risk, combined with overly rigid and onerous new requirements, could act as a headwind to investment and innovation, and potentially place the EU at a global disadvantage. This is particularly the case with a stringent ex-ante

oversight and approval mechanism such as that proposed, which necessitates significant time and resources for both regulators and businesses, and could be especially detrimental for the competitiveness of SMEs in particular. Legal certainty of key concepts is extremely important for companies to manage their risk and comply with regulation appropriately. Several such concepts in the paper are not sufficiently well defined to provide legal certainty and could result in paralysing development in certain valuable areas. In particular, we would wish to see clear, detailed legal definitions of 'significant risk', 'likelihood' and 'exceptional instances', as well as the removal of the category of 'immaterial damage' (which is also largely covered by other laws such as data protection, non-discrimination and freedom of expression).

Risk governance and industry best practices

Finally, when assessing risk (and by implication governance) we would ask that the Commission take into account the significant, rigorous measures organisations may already have in place for the development of AI. Clearly all firms have a responsibility to continue to improve and invest in these processes and frameworks, but not all businesses are starting from the same place today. It may not be a productive use of resources to consider all cases falling into the high-risk category as comparable, when some have undergone (or will undergo) significantly more internal oversight and governance than others.

As discussed in Sections 2 and 3, Visa is acutely focused on the need to build and maintain a social license to operate in this space through consistently trustworthy, explainable practices. For this reason, our use of data and data-driven technologies is governed by several layers of governance and risk management. For illustrative purposes, our MRM process today defines and manages Visa's overall risk-based approach, including awareness of model capability and use, proper controls, monitoring, escalation, and accountability. MRM specifically drives independent validation and solid governance of business-critical models, whether developed internally or externally. Visa is currently evolving our MRM approach, clarifying the roles and responsibilities across the Three Lines of Defence Risk management approach and throughout the model lifecycle. We are also creating a central model repository, standardised procedures and templates, and governance by model risk tier along the materiality / (un)certainty matrix discussed above. Our aim is for 50% of medium risk models to undergo independent validation by next year, with a stretch goal of 100% high-risk models. MRM exists in addition to Visa's Global Privacy Program; a specific operating framework for data (the 'Data Use Principles'); the Data Use Council (a pipeline evaluation body for specific use cases of data); the Data Council (a panel of senior executives responsible for strategic oversight of all data-related activity); specialised training and workshops.

We will continue to invest in these risk and governance processes for the benefit of consumers, our clients and our business. It would seem practical for a new targeted, risk-based regulatory approach to take into account a high standard of oversight within the relevant organisation, and to ensure compliance processes complement, rather than complicate or impede, existing internal frameworks.

8. Regulatory requirements, compliance and enforcement for high-risk applications

Properly and proportionately designed on the above principles, we would expect the use cases falling into the high-risk category to be relatively few and extremely clear. This is commensurate with the Commission's goal to target 'problem areas', while still allowing for the flourishing of innovation where the risks are relatively low, as they should be in the majority of cases. Once again, we would reiterate that although Visa supports the need for new governance to mitigate risks posed by AI, this is appropriate only where other existing regulation cannot adequately do so.

Conformity assessment test

As discussed in Section 5, as a general principle for technology regulation, Visa believes there are limitations to the suitability of process-based, ex-ante regulation in this area. Therefore, while we support the Commission's aims to minimise risk, we believe it is important to ensure that the proposed process of prior conformity assessment does not duplicate existing self-assessment frameworks and is designed in a way that is practical and effective for both regulators and industry participants. Any new process should be aligned with industry standards and best practices. Assessments should aim to avoid becoming an onerous "tick-box exercise", and should not replace best-in-class industry approaches, but instead offer guidelines and be a practice that adds value to the overall ecosystem.

Harmonisation and alignment with industry standards

We would also strongly recommend that any suggested framework be closely aligned with internationally recognised standards. Notwithstanding the need for diversity of organisational approaches (for example to cater to different business models, sectors, use cases), standards help to outline the technical and organisational means to comply with regulatory requirements. Harmonisation with standards would help to ensure efficient, streamlined compliance with the requirements of conformity assessments, benefitting both industry and regulators.

Ex-post conformity assessment test

Alongside the prior conformity assessment, the White Paper envisages a role for market surveillance and ex-post controls, including the production of documentation and testing, where appropriate. Where needed, and conducted in an efficient, proportionate matter, these mechanisms (such as scrutiny or auditing of risk impact assessments) could usefully limit the possibility of bottlenecks in the prior-conformity process, ensuring resources are spent where need for prior conformity assessments to the most high-risk cases. This would reinforce the expectation of reasonable scrutiny across the wider market, while avoiding impeding fast-moving development where this is not strictly necessary.

We welcome the Commission's statement that any new mechanism will be "proportionate, non-discriminatory and use transparent objective criteria in compliance with international obligations". A number of measures could be taken to facilitate this. Stakeholder engagement and open channels of communication are key, and it is commendable that the Commission recognises this as an essential part of this process. Regulators will require the expertise and resources to be agile, responsive and time-efficient to avoid bottlenecks. The ability of regulators to respond to cases should be regularly reported and reviewed, with frequent opportunities for feedback and adjustment where required. Fast-tracking or 'compliance lite' processes should be considered in cases with clear precedent or comparability. Similarly, cases with clear urgency should be permitted to apply for priority assessment. Sandboxes or other forms of collaborative development could be helpful in guiding novel use cases where the application of the law is not yet clear.

Types of requirements for trustworthy AI

The features suggested in Section D of the White Paper are all sensible considerations for building responsible AI and it is welcome that these features build on the work of the HLEG and on the principles of the GDPR. It is also well understood that properly embedded and documented processes are critical to building responsible AI, and that these can assist regulators in understanding how accountability, legality and ethics are managed. The Commission's recognition of the need to protect confidential commercial information, such as trade secrets, is extremely welcome. Infringement of this would be a significant demotivator for AI investors in the EU. Notwithstanding the importance of proper record-keeping of data and other elements of AI development, regulators should remain cognisant of the cumulative effect such requirements have on organisations, in particular those with fewer resources to expend on supporting these processes. Where requirements such as those in Section D are already covered under existing law, we would not expect to see duplicative action

required. The onus to address and streamline any overlaps (or contradictions) should rest on regulators, not on industry participants.

Bias and human oversight

Regarding human involvement, as the Commission notes, the appropriateness of this will vary case to case. However, it should be noted that the degree of human oversight is not always a useful indicator of risk nor the most effective tool to mitigate harm. Humans can be the cause of bias built into models, and human oversight by a biased or non-competent implementer could result in a greater, rather than lesser, degree of risk. We recognise the Commission's concern regarding the potential for a model to evolve over time and thus potentially require a fresh assessment. However, this should be limited to a clear definition of 'material changes' which properly reflects the impact of a simple change such as a security update, for example, versus that of a substantial change to the functionality or purpose of the product that alters the potential for harm.

Retraining of data and models

Visa is particularly concerned by the Commission's proposal that AI systems may be required to be retrained in the EU, or using EU data. We understand the need to meet the applicable requirements within the EU. However, we do not see the proposed remedy as either an appropriate or an effective way to address the issue. Using broad, diverse sources of data is critical to effective combatting of fraud and cybercrime. It is also a powerful tool to mitigate bias and unlawful discrimination. Limiting or specifying which data may be used to train a model on the basis of regional provenance risks hampering the ability of businesses to protect the online world and exacerbating, rather than limiting, the risk of bias and discrimination. It also represents an extremely unwelcome move toward data localisation, to which the Commission emphasised its opposition in the European Strategy for Data. The EU has played a leading role in advocating against localised restriction of data flows and other protectionist measures related to storage and systems. We are encouraged by the Commission's expressed intent in the Strategy to continue to do so.

9. Voluntary certification and labelling for AI Applications

Visa is optimistic about the potential of a voluntary certification and labelling scheme for AI applications not deemed high-risk. Such a scheme (applied in the appropriate cases) could help drive best practice, enhance consumer trust in new products in the marketplace, and familiarize organisations with the sorts of principles and processes required to build trustworthy AI. However, we

would query the logic of imposing the same stringent legal requirements designed to mitigate the risks of high-risk AI to a voluntary scheme aiming to mitigate low-level risk. This potentially disincentives participation (particularly from smaller companies without resources to participate in an onerous process) and may create the same bottlenecks and delays which are possible under the high-risk regime. A balance must be struck between a regime robust enough to merit accreditation (and thus trust) and the commensurate level of risk attributed to these applications. It would be useful to explore similar industry-driven certification schemes, for example those available for IoT device security. These schemes exist to serve different industry needs, depending on the respective risk level and risk appetite. This could potentially be an alternative to one single scheme.

The HLEG Trustworthy AI Guidelines address the potential for harm through establishing strong ethical foundations for AI. Anchored in good governance, best practice and international standards, the Guidelines aim to drive the acceptance and embedding of principles and practices which go beyond legal compliance, assessing trustworthy AI through the lens of ethics, rather than law. These were compiled and tailored to the AI development process through broad participation, with support from industry, and Visa believes they are already helping to drive AI developers to shape internal governance structures appropriately. Whilst the Guidelines themselves were rightly not intended to comprise a prescriptive checklist of process requirements, Visa would encourage the Commission to instruct further work from the HLEG to define a clear criteria and a methodology for evaluation and assessment of AI applications under the voluntary scheme. The HLEG's expertise and consultative framework for such a project is now well-established and much foundational work already in place.

10. Addressees

The Commission's proposal states that obligations in respect to legal requirements should be addressed to the actor best placed to address risks arising at different points in the development and implementation phases of AI.

Visa supports the need for effective safety and liability frameworks to protect against any new risks that emerge for users of AI systems. Visa supports the Commission's proposal that obligations in respect of legal requirements outside of the Product Liability Directive (and other areas of law) should be addressed to the actor best placed to manage risks arising at different points in the AI lifecycle. Visa has emphasized this point in various recent regulatory submissions and we would emphasise again here the importance of clarity over addressees for the purposes of ensuring proper apportionment of risk, liability and consumer redress. Regulation or guidance, which does not clearly specify addressees, risks liability falling between the gaps or being inappropriately assigned.

For example, Visa is a developer of data-driven models, some of which would potentially be classified as AI under the definition above. In most cases, we are not a Data Controller, do not implement automated decisions, and do not hold direct relationships with consumers. We develop models for our clients (largely banks, but increasingly also merchants) who use these models either in whole, or as part, of a decision-making process. In this scenario, we would describe the client as the deployer. Depending on the degree of human involvement, within the client will sit personnel responsible for using the model in a decision instance. This group might be described as implementers. In addition to having no direct interaction with consumers, the nature of the data Visa holds means that in the vast majority of cases we do not even know who the data subject / decision recipient is. There will therefore be several key elements of the process over which Visa has less (or no) oversight or control. This is well reflected in the Commission's statement that the ability of developers to control risk during the use phase may be more limited.