Treasury

# A Strategic Plan for the Payment System

## Submission of Lockstep Consulting

George Peabody & Stephen Wilson
Lockstep Consulting
February 2023

**FOR PUBLIC RELEASE**

Government submission

**A Strategic Plan for the Payment System: Submission of Lockstep Consulting**

For The Treasury

[Lockstep Submission - Treasury - Strategic Plan for the Payments System 230201]

George Peabody & Stephen Wilson

ABN 17 582 844 015

**FOR PUBLIC RELEASE**

*Lockstep Consulting (est. 2004) provides independent research, analysis and advice on digital identity, privacy and data protection.*

https://lockstep.com.au

# Introduction

**Lockstep** (est. 2004) is an independent Australian-owned research firm providing offers vendor-neutral research, analysis, strategic advice and policy consulting, to help organisations break through data and identity management challenges. Lockstep is expert in:

- data protection and verification, in respect of technologies and global regulations
- data privacy
- digital identification
- global payment systems
- Privacy Impact Assessment (PIA), Threat & Risk Assessment (TRA)
- smart and autonomous technologies (mobile credentials, smartcards, PKI and cryptography) and
- the verticals of government, e-health and financial services.

Our response to the payments system consultation is informed by our work at the intersection of payments and digital identity, where we research the challenges of data protection and help develop progressive approaches to security and customer privacy.

See also https://lockstep.com.au.

**George Peabody** (Principal Consultant) is a 20-year veteran of the payments industry. With 30 years in IT-based entrepreneurship and product management, he has expertise in payments strategy and market development. His interests range across business and technology areas including mobile and POS payments acceptance, online and offline data security, and data verification. Before joining Lockstep, George was partner at payments industry consultancy Glenbrook Partners. He has led telecommunications research teams. He co-founded payment *identity firm Payment Pathways* and a regional ISP. George produced and continues to co-host *Payments on Fire*®, the top-rated payments industry podcast.

**Stephen Wilson** (Founder and Principal Consultant) is an international authority on data protection, digital identity and privacy. He has helped organisations around the world with independent advice and analysis in technology & governance strategy, business architecture, privacy, risk management, Privacy Impact Assessment and public policy. He is a widely respected writer and commentator on all issues relating to digital identity. His career spans 35 years in IT, software engineering and R&D management, in both Australia and the USA, with 25 years dedicated to digital identity and privacy.

## About this submission

This document is structured to address the seven numbered questions set out in Treasury's consultation paper *A Strategic Plan for the Payment System*, December 2022.

We confirm that we understand submissions will be made public.

## Contact

Lockstep is happy to discuss any aspect of this submission further in any forum, and to support Treasury progress the strategic plan.

Please contact us via Lockstep's Managing Director:

Stephen Wilson
[redacted]
[redacted].

## Abbreviations & Acronyms

| | |
|---|---|
| AML | Anti-Money laundering |
| API | Application Programming Interface |
| APP | Australian Privacy Principle or |
| APP | Authorised Push Payment |
| APPlus | Australian Payments Plus |
| CBDC | Central Bank Digital Currency |
| CDR | Consumer Data Right |
| CIAM | Consumer Identity and Access Management |
| CRM | Customer Relationship Management |
| DTA | Digital Transformation Agency |
| DVS | Document Verification Service (now known as *IDCheck*) |
| NFC | Near Field Communications |
| NPP | New Payments Platform |
| PAN | Primary Account Number (esp. of a credit card) |
| PKI | Public Key Infrastructure |
| PSRA | Payment Systems (Regulation) Act |
| RBA | Reserve Bank of Australia |
| SME | Small to Medium Enterprise |
| TDI | Trusted Digital Identity (of the *DTA's* draft legislation) |
| TDIF | Trusted Digital Identity Framework |

# Stakeholder questions and Lockstep's answers

## 1. What are your views on the proposed key principles?

Are there other principles that should be included?

We believe there are additional design and market structure principles and concerns necessary to support the key principles.

### Expand the Scope of the Payment System Strategy

A singular focus by Treasury on payment system strategy is too narrow to meet the long term needs of the nation. The broader domains of financial services—exemplified by the open banking movement—should fall under the nation's payments strategy.

From a market development point of view, separation of payments from other financial services reinforces the traditional market model at a time when innovation is taking place across domains and lines of business. For example, third party payments providers now often include lending in their offerings via, for example, *buy now pay later* services. Treating them as separate concerns or as specific payments use cases assures regulatory confusion for market participants (which may be exploited by certain participants) and, as innovations and new use cases arise, will make it difficult for regulators and the market to respond to the inevitable demand to shoehorn these efforts into a regulatory framework that never anticipated such changes.

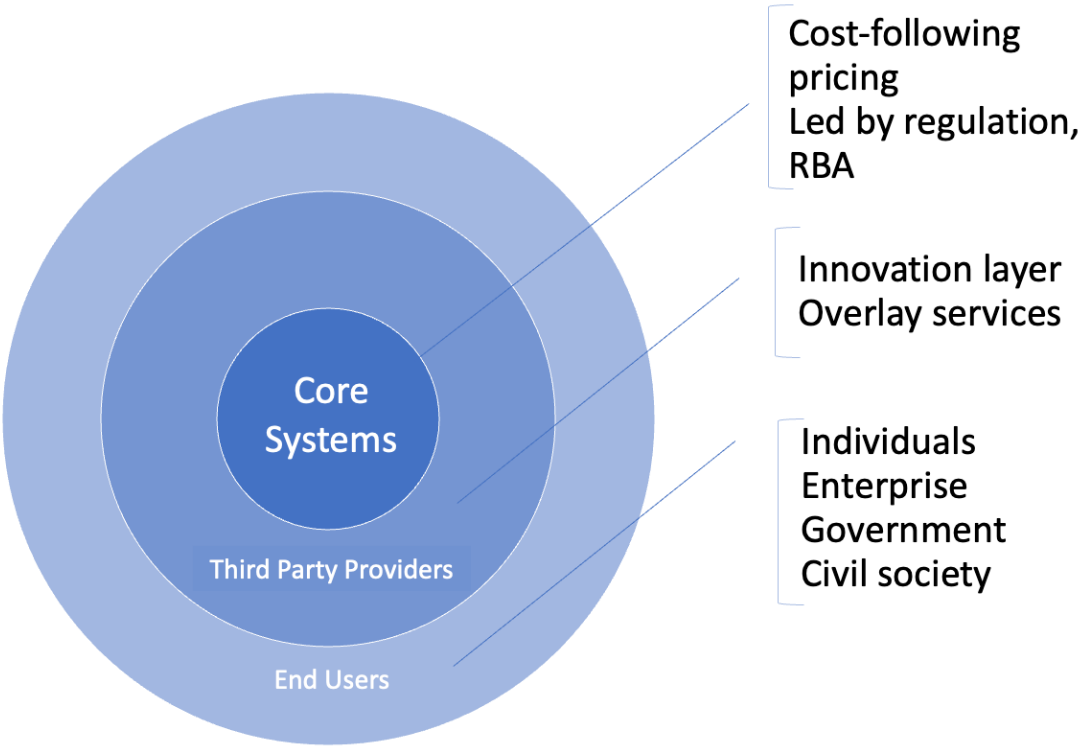
In other words, the Treasury's proposed approach seems insufficiently flexible to accommodate long term needs. Expansion of the inter-agency payments forum work should include open banking, CDR, identification standards, and secure data management. We suggest consideration be given to consolidating government agencies concerned with payments.

### Core System Goals

Experience shows other countries—especially India and the U.K.---have benefitted from applying critical infrastructure perspectives to national payment system design and operation. Across all methods of payment—wires, batch, cards, retail real-time push payments (in Australia, the NPP) and cryptocurrency—regulatory goals should be based on cost-following, utility-grade models. In some cases, this might include payment system operation by the RBA or its contractor. In other cases, usage cost and participation access may be governed by regulation alone.

The goal of this approach is universal access to these services for end users and market predictability for third party providers who use and/or expose payment system capability to their customers.

From a government-level, their operation and cost structure are foundational to the principles of efficiency, innovation, accessibility, and trustworthiness. Therefore, it is in the nation's interest for the government to focus on these core systems as critical infrastructure and platforms for innovation for the widest possible participation in the economy.



## 2. What are your views on the proposed key priorities?

**Do they provide enough certainty on what the key priorities are for the Government? Are there other matters that should be included?**

## Promoting a safe and resilient payments system

With respect to online identification, authentication and cybersecurity, there is significant tension between the demands of privacy, security, legitimate surveillance, and surveillance capitalism.

We believe that the current methods of online identification are inadequate and have demonstrably failed to prevent data breaches and data misuse. We believe a new model of data verification is required so that Know Your Customer protocols can use better quality data resistant to theft and fraudulent replay. Simply throwing more "identity" at the spiralling problems of data breaches and synthetic identities will not work, for it only incentivises the criminal trade in stolen data. Some pundits have faith in an all-new digital identifier, but even if that could be engineered to be *guaranteed* resistant to theft, it would impose enormous unbounded switching costs on business, and face political risk of consumer rejection.

Lockstep has researched an alternative verified data sharing model, which we present for discussion (see attached).

## Ensuring fit-for-purpose regulation and competition

Every effort should be made to develop a single national set of regulatory requirements for all financial services actors, with role-specific extensions and modifications. To accomplish this, regulators need to crisply define their remit and the relationship of their domain to adjacent regulatory bodies. State-level rules should be minimised where possible.

This level of alignment encourages innovation and competition. New fintechs and older incumbents alike hesitate to invest in new services and back-office upgrades when regulatory overlap, uncertainty, or lack of clarity exist. Fintechs are hesitant to deploy their limited resources while regulations are under development. Incumbents often have limited incentive to innovate, as they continue to benefit from the status quo.

Again, agency consolidation is worth examining.

## Alignment with broader digital economy transformation

Digital and economic transformation are essential components of the payments strategy. Open banking, CDR, improved online identification, and the impact of the more mainstream cryptocurrency developments (such as stablecoins and CBDC) all resonate with payments. A holistic review of those developments will strongly support the fitness-for-purpose of the regulatory framework, foster proper standardisation, and promote competition.

## Modernising payments infrastructure

This priority is fundamental to the success of the overall strategy. A modern payments infrastructure is a national asset and core competency. It is the *sine qua non* that enables other priorities and initiatives. Modern core systems should be cost-following services for the good of the nation. Let industry innovate and provide value on top of Australia's modern payment rails.

*Note that we find it more coherent to address questions 3 and 4 together.*

## 3. What are your views on the proposed supporting initiatives?

## 4. Do you have any feedback on the proposed approach?

We offer detailed feedback regarding fraud, cybersecurity, regulation, transparency, costs and competition.

## Reduce the prevalence of scams and fraud

Fraud modalities are shifting. For one thing, physical identity documents are rarely counterfeited today to perpetrate fraud; instead, most identity crime is now done by copying identifying details from large data breaches and using them to impersonate people online.

Similarly, scammers know it is often easier to convince their victims to send them money than it is to take over an individual's account to access funds. Authorised push payments (APP) exacerbates these social engineering attacks, because the fraud is difficult to detect prior to the victim sending money and ex post facto remediation is expensive and uncertain.

### Accountholder Education

We believe a consistent, required program of customer education does add a measure of consumer protection. The U.K. and multiple mobile network operators providing mobile money services have done a credible job of warning consumers about the scammer danger. Bad experiences have created a "sadder but wiser" mindset among many users of these systems.

That said, there are limitations to the effectiveness of user education. Despite a strong awareness program, the U.K.'s APP fraud losses now exceeds its card fraud losses. Education alone won't fix it.

### Risk and Cost Allocation

In the case of scammed customers using person to person push payment methods, putting the remediation burden exclusively on accountholder banks through mandated ePayments Code compliance is, no doubt, an attractive, quick fix remedy for regulators.

However, these push payment transactions are by design, from the consumer and bank's perspective, low cost and low margin, respectively. That low cost is a contributor to innovation. Banks, if mandated to make good victim's losses, will be forced to live with a very low profit or loss-making service. Given bank competition, it will be impossible for a single bank to raise its fees to cover the ongoing losses of their defrauded accountholders. In other words, something has to give and simply shifting liability among the actors using existing procedures is not a sustainable solution.

The problem cannot be cured via a liability shift entirely to the financial institution because both the financial institution and its accountholders have insufficient information to detect possible fraud.

For example, we believe the party that owns the risk, the accountholder sending the money in the P2P case, has insufficient information to determine the trustworthiness of the recipient of their funds. To provide the sender with more information, we believe banks and PSPs need access to the "story of the data," beyond simply what is stored in a directory, and to report their findings, in aggregate, to the sender.

Examples of this metadata include:

- the creation date and age of the email address provided
- the extent of the email address's use
- the age of the mobile number's account
- the physical address associated with the mobile number
- a signal telling how the mobile account was onboarded and what KYC steps were taken
- the usage pattern of the destination account (an increase in deposits and payments for example might indicate the destination account belongs to either a scammer or a mule employed by the scammer).

These, and other, verified credentials provide greater power to the service provider to discern between legitimate and fraudulent activity. The service provider might send a message to the sender before payment initiating indicating whether or not the destination account is trustworthy. A "thumbs up, thumbs down" emoji could provide the sender with a strong signal to encourage, at least, caution. If the sender chooses to proceed after receiving a "thumbs down" signal, the service provider could make the case that transaction liability should shift to the sender. The ePayments Code would codify the liability shift.

Such verified credentials would also mitigate the problem of synthetic identities confronted by banks and fintech services onboarding new accounts and performing KYC functions.

## Strengthen defences against cyber attacks

The habitual over-collection of personal and business data by information-hungry service providers has made corporate data resources all the more attractive to hackers. Regulations and data sharing models that discourage such data collection are critical. Mandated data minimisation and protections for the data that is stored, e.g. encryption and tokenisation, may be appropriate.

At the same time, a mature defence-in-depth security culture recognises that data breaches will never be stopped entirely and that there are many legitimate reasons for certain personal information to be recorded. So, a balanced data protection approach will also do more to reduce the risks posed by stolen data. We strongly advocate transaction signing and verifiable credentials to provide proof of possession and tight control over data presentation, to make data replay by fraudsters far harder than it is today.

## Supervision of systemically important payment systems

We encourage an activist approach to the guidance and management of systemically core systems. The key principles are best served by direct RBA oversight of utility scale, cost-following payment rails.

## Implement changes to the PSRA 1998

We suggest writing the regulatory update from the perspective of an implementer providing services in 2033. While anticipating the exact form of the future is impossible, technology-driven change requires a responsive regulatory framework.

## Introduce a payments licensing regime

Tiered provider licensing is a practical means to enforce specific regulatory requirements given the unique and fine-grained distinctions between fintech services. Licenses should go beyond payments alone to accommodate the expanding range of financial services and how they are brought to market. These licenses should apply to all financial services, not just access to payment data or payment initiation.

### Enable greater collaboration between payment system regulators

We believe consideration of consolidation of payment system regulatory agencies and, as stated, expansion of its remit beyond payments is worth examination. Alignment without structural incentives equally applied is very challenging.

### Promote competition via transparent access to payment systems

As stated, we believe a core and overlay approach is important. The RBA has direct oversight implemented through mandate or influence over core system development and operations based on a utility model of payments. Third party providers of all kinds, subject to fine-grained licensing requirements, expose the capabilities of the core systems to market and add value through innovation and use case specific solutions.

### Reduce small business transaction costs

Regarding merchant discount fees, it is important for regulators to take into account the value delivered to SMEs by their service provides above and beyond the payment itself.

Traditional merchant acquirers and their channel partners only delivered card acceptance and ancillary services such as terminal leasing. Today's fintech-based service providers deliver significant value over and above payment card acceptance alone for rates that are competitive with the traditional providers. Vendors like Block's Square service, for a single, admittedly blender rate, bring simplicity, convenience, an improved user experience, and valuable new capabilities to their SME customers. This simplicity and improved users experience for both customers and SME staff (little to no training required) have business value.

A hard focus on SMB payment costs when compared to large enterprise acceptance costs may miss the value delivered by some fintechs. The proposed strategy's key principles of efficiency and innovation would be violated should regulations not take overall value delivery into account.

## 5. What are the key milestones for key initiatives that you would like to see included in the Plan?

**Are there any conflicts between milestones or pressure points that need to be taken into account in revising the roadmap?**

We believe regulatory alignment, even consolidation, across payments, open banking, CDR, identification, etc. is a first order priority and should be moved ahead in the roadmap. Discussions and coordination are inadequate. Privacy and security are design time concerns; retrofitting systems to meet new requirements is impractical.

## 6. What are your views on the proposed review process and engagement arrangements?

No comment.

## 7. Are there any other sections or topics that you would like to see added to the Plan?

No comment.

# Attachment

Lockstep is researching and designing a new business model and architecture for sharing verified data and quality signals. Such a capability is central to the developing digital economy, and is increasingly an explicit feature of business and government reform agendas. Informed by our extensive research and client-facing work in international cybersecurity, privacy, digital identity and verifiable credentials, we have tried to capture most of the contemporary requirements for enabling orderly data sharing at scale.

We believe *verifiable data sharing* will supersede current concepts of digital identity, digital credentialling, identification, and "trust frameworks".

Our vision for a unified global architecture for verifying and sharing data has particular potential in payments system transformation, and so we offer for discussion the following executive summary of a soon to be released paper.

## A new Data Verification Platform

**We propose a general unified model for verifying data which uses the latest techniques for sharing verifiable credentials in a general-purpose network business model.**

Open data, open banking, the rights of access to publicly funded research, and so many other plans to "unleash the power of data" are being promoted across government, business, and social institutions. But what do we know about this data? For starters, how do we know any data is legitimate? And how can we know the important finer-grained properties such as the jurisdiction of origin, the algorithms used in processing, and consent to share?

There is clearly a need for all organisations to be able to verify the data they're relying on.

To achieve these lofty data-sharing goals, we need an environment which is both orderly and scalable. The users of data need to be reassured about its quality, its provenance, the permissions for its use, transparency about the processes that created it, and more.

Developments in the digital identity industry are instructive. With ever more emphasis on provenance, authority, fidelity, privacy, and agency, the parties to a transaction are focusing on credentials, affiliations, and other attributes — in other words, the metadata surrounding traditional "identity" data such as date of birth or national ID numbers.

In both the FIDO Alliance and in verifiable credentials, “identity” is less prominent, or even absent altogether. This is progress.

The data structures and signatures which are already being used for verifiable credentials can be broadened beyond personal identity and related attributes. A verifiable credential is, in fact, an attestation by a respected source about a fact about a subject — and that could be any fact. Indeed, it could be an attestation to any facts about anything, including non-human subjects, IoT devices, and data more generally.

But that raises another question: How do we scale up the acceptance of verifiable credentials and data when the entities who rely on the data are distant from the data’s origins, whether that’s geographically or legally? How do they know they can trust the entity making these attestations?

Data verification requires more than just technology. It also needs an infostructure that includes global rules and scalable processes for distributing meaningful facts. We have researched and designed an infostructure to bring the users and originators of data together under a uniform set of platform rules so that they can interoperate without needing to negotiate bilateral legal arrangements.

**We set out here a data verification platform (DVP) which provides the operating principles and core functions needed for trustworthy data and credential sharing.**

The platform intermediates the communication of verifiable data about data subjects between the sources of facts, the data origins — which may be government entities, institutions, enterprises, manufacturers, supply chain members, media companies, content creators, or business intelligence providers — and the risk owners who use those facts, via new types of specialist businesses we call data distributors.

Our proposed model deploys verifiable credential tools in what economists call a two-sided market, where all the parties’ risks and roles are aligned economically and standardised contractually — a characteristic lacking in existing systems of federated identity.

Our DVP provides a common foundational ruleset, regulatory posture, legal arrangements, certification framework, secure message routing, uniform UX requirements, and trust mark branding. It ensures that when one party requires data about a counterparty to carry out some transaction, that data can be obtained from reliable sources, supported by a range of verified quality signals which are aligned with the risk-management needs of the transaction risk owner.

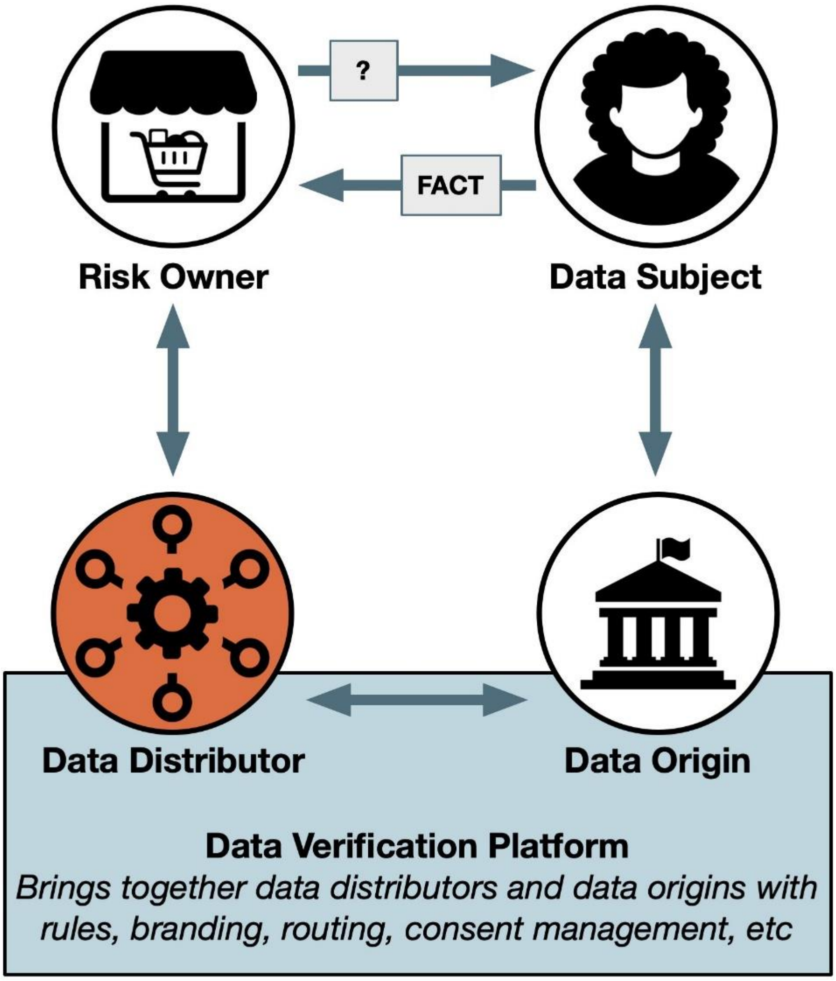

?
FACT
Risk Owner
Data Subject
Data Distributor
Data Origin
Data Verification Platform
Brings together data distributors and data origins with rules, branding, routing, consent management, etc

**Figure 1: High-level DVP architecture**

The DVP model fosters the fine-grained definition of transaction data, data sources, and verification metadata. All this information will be available in the DVP ecosystem to the designers of transaction system so they may build in comprehensive real-time data verification.

**We deliberately use new terms to clarify the essential functions and roles of each party using DVP-mediated data.**

To explain further, in our generalised data-sharing model the central parties are the data subjects and risk owners. The risk owner is typically the first party to a transaction in which services are provided to a data subject or second party. To manage specific risks, the first party always needs to know some data about the second party, and that data usually has a defined or preferred origin(s).

The DVP supports risk owners in obtaining verified core data about subjects — in plain language, facts — plus metadata about each fact's reliability, at scale, from diverse sources using standard data verification protocols.

Verifiable facts originate from participating authoritative data origins. And the new players, the data distributors, make these facts more reliable and more easily discoverable across the DVP network by onboarding the risk owners with a set of consistent legal agreements and technology with which to connect to the DVP network.

**The DVP is about delivering the facts, direct from the source, including the metadata that tells the story of that fact, to the risk owner, with fine-grained quality signals to use for crisper risk-based transaction decisions.**

The DVP does not alter any fact, yet it makes the data better. The DVP makes a rich array of quality signals available to any party that relies on facts, so that the facts are more reliable. As a result, transacting parties can make better, faster, lower-risk decisions based on those facts. One major beneficial side-effect will be that businesses can cut down the amount of ancillary data they collect about the subject, because the core data they really need know will be so much better.

In the DVP ecosystem, the risk owner's application can be designed in advance around specific data and metadata available from associated data distributors, so that the optimum verifiable credentials are available in real time for each transaction type, to support risk-based processing decisions.

The risk owner receives from the data distributor a unique, DVP-mediated set of data containing core and contextual facts and the associated metadata for each, all timestamped and signed at the source.

Building the DVP will be a heavy lift, but comparable efforts have succeeded and indeed thrived in time.

By way of comparison, the payment card system has enabled a globally accepted payment and user experience through its founding principles, architecture, standards, business model, and contractual consistency. As one of the first true two-sided markets for digital services, the card system has delivered enormous value for merchants, consumers, and financial institutions, and fostered countless fintech businesses.

The FIDO Alliance is a fine contemporary example of collaboration on global security standards by competing risk owners, including banks, telcos, insurers, e-commerce and mobile platforms, security vendors, and big tech.

For both FIDO and the card schemes, the foundations for global scalability are their common principles, transparency, and respect for the needs of all participants.

The global card system has produced a secure yet simple to use system of Click to Pay, already in use in many countries. Our DVP can similarly produce a secure yet simple to use system of "Click to Prove", so that any attested fact about you can be held safe in a mobile wallet and presented by you, in-app, to a counterparty, easily, privately, and securely.

**Building a global data platform can be done again. Indeed, a modern general- purpose platform must be created in the interests of properly governed, economical, and uniformly experienced data-sharing worldwide.**